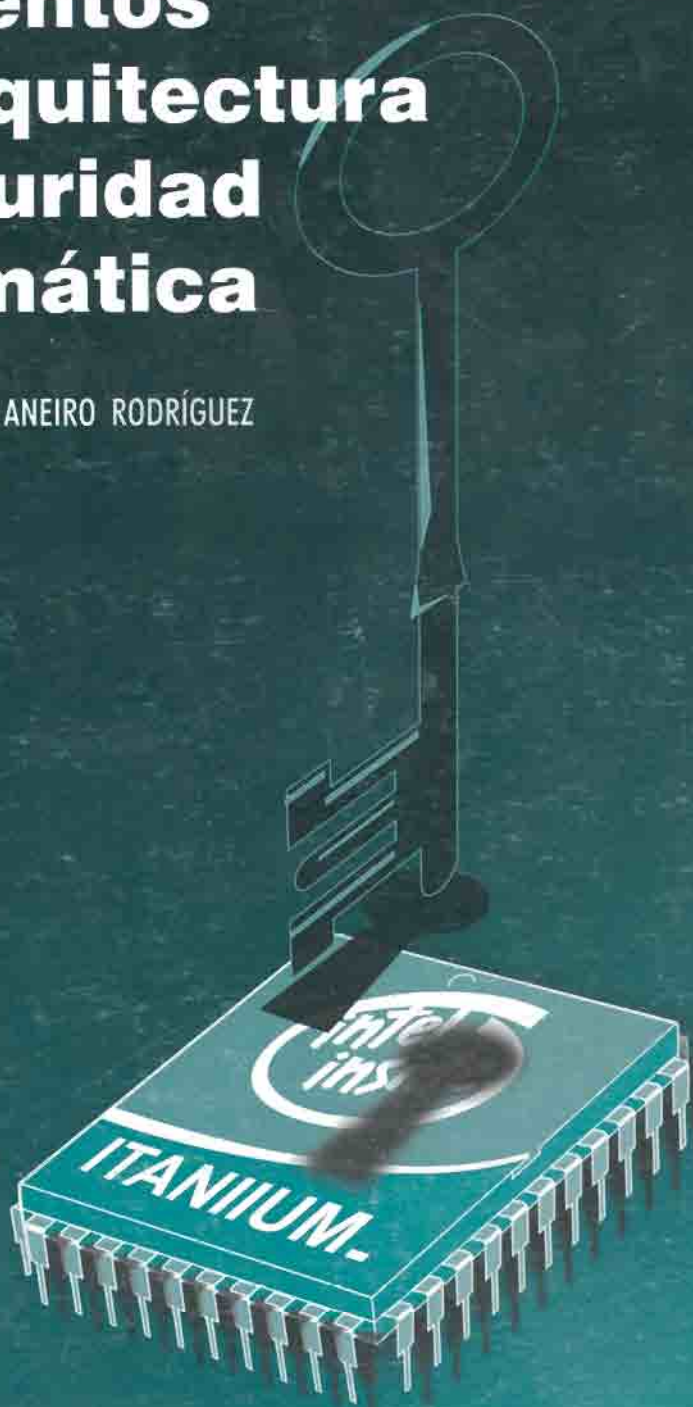


elementos de arquitectura y seguridad informática

LÁZARO ORLANDO ANEIRO RODRÍGUEZ



Diseño de cubierta: Alberto Cancio Fors

© Lázaro Orlando Aneiro Rodríguez, 2001
© Editorial Pueblo y Educación, 2001

ISBN 959-13-0819-1

EDITORIAL PUEBLO Y EDUCACIÓN
Ave. 3ra. A No. 4605 entre 46 y 60,
Playa, Ciudad de La Habana,
Cuba. CP 11300.

A nuestros lectores

El libro Elementos de Arquitectura y de Seguridad Informática ha sido concebido por profesores de Computación del Instituto Politécnico Eduardo García Delgado y de la dirección de Computación Educativa del Ministerio de Educación.

Es, en esencia, un libro de texto para los politécnicos de informática en nuestro país, dirigido a estudiantes y profesores, de forma que unos y otros puedan contar con una herramienta importante para el desarrollo del proceso de enseñanza aprendizaje de la Computación. También puede ser empleado en los institutos superiores pedagógicos y preuniversitarios como una fuente cultural para los profesores.

Cada uno de sus capítulos tiene cierta relación de dependencia con los precedentes, es decir, se evitan repeticiones de conceptos que hayan sido abordados, sin que esto implique, necesariamente, la lectura secuencial de los contenidos.

Por otra parte, no constituye un manual de referencia y aunque su contenido tiene actualidad, por el propio desarrollo de estas tecnologías se recomienda la consulta de otras fuentes. Por otro lado, muchos de los aspectos que consideramos importantes, no se han mencionado y por ello, pedimos disculpas a todos los lectores potenciales de este libro.

Pretendemos que los estudiantes encuentren información sobre los elementos básicos para el aprendizaje de cada uno de los temas y, al mismo tiempo, la necesaria orientación, para de forma independiente, incursionar en los aspectos no abordados.

El autor

Tabla de contenidos

I. INTRODUCCIÓN A LAS COMPUTADORAS	6
INTRODUCCIÓN	6
RESEÑA HISTÓRICA DEL DESARROLLO DE LA COMPUTACIÓN	6
CLASIFICACIÓN DE LAS COMPUTADORAS	8
TIPOS DE COMPUTADORAS	10
¿QUÉ ES UN MICROPROCESADOR?.....	11
II. TARJETAS PRINCIPALES DEL SISTEMA EN LAS PC	32
LA MEMORIA	32
MEMORIAS DE SOLO LECTURA	36
AREAS DE MEMORIAS EN LA PC	38
PROCESO DE ARRANQUE	53
EL BIOS	56
CHIPSET	67
MEMORIA RAM Y TIEMPOS DE ACCESO.....	102
UNIDAD CENTRAL DE PROCESAMIENTO (CPU)	113
CACHE	113
III. MICROPROCESADORES AMD Y CYRIX 6X86	121
AMD	121
EL OVERCLOCKING	133
RELACIONES DE MULTIPLICACION DEL MICROPROCESADOR	136
IV. TORRES DE DISCOS Y OTROS MEDIOS DE ALMACENAMIENTO	146
DISQUETERAS	146
DISCOS DUROS	146
CONTROLADORAS DE DISCOS DURO	153
ESTRUCTURA LÓGICA DE LOS DISCOS DUROS	155
TORRES IOMEGA (MO, ZIP, JAZZ).....	156
CD Y DVD-ROM	157
DISPOSITIVOS DE DISCO COMPACTO.....	159
EL DVD: ¿UN NUEVO ESTÁNDAR?	160
V. TARJETAS DE EXPANSIÓN E INTERFACES	167
CONECTORES: PCI, AGP... ..	167
TARJETA DE RED	173
EL USB.....	178

VI. TRATAMIENTO DE LOS FICHEROS DE SISTEMA Y SU EXPLOTACIÓN.....	180
WINDOWS Y LA MEMORIA VIRTUAL.....	180
VII. EQUIPOS PERIFÉRICOS ASOCIADOS.....	184
PUERTOS SERIES (UART).....	184
PUERTO PARALELO.....	185
TECLADO.....	185
¿QUÉ ES... UN ESCÁNER?.....	188
EL MOUSE.....	193
¿QUÉ ES... UN MONITOR?.....	196
¿QUÉ ES... UNA IMPRESORA?.....	204
VIII. SEGURIDAD INFORMÁTICA.....	216
SEGURIDAD DE LA INFORMACIÓN.....	216
SEGURIDAD FÍSICA Y LÓGICA.....	217
DEFINICIÓN Y TÉRMINOS DE PROGRAMAS DESTRUCTORES.....	227
ANEXOS.....	241
ANEXO 1: DICCIONARIO DEL HARDWARE.....	241
ANEXO 2: SETUP.....	259
BIBLIOGRAFÍA CONSULTADA.....	299

I. Introducción a las computadoras

Introducción

Los grandes avances en la ciencia y la técnica logrados por la humanidad, en todas las ramas de la producción y los servicios, no se conciben sin la participación continuada y creciente de los recursos informáticos y computacionales, los cuales debido al acelerado desarrollo de nuevas tecnologías aplicadas en la electrónica, han evolucionado, perfeccionado y aumentan cada vez más en potencialidad.

Reseña Histórica del desarrollo de la Computación

Blaise Pascal (1623-1662). En 1642 inventa la máquina de engranajes. A medida que iban girando los engranajes se producían los cálculos. Una máquina que necesitaba energía para funcionar.

Leibniz (1646-1716). En 1694 inventa la calculadora que usa el sistema binario.

Josep Jacquard (1752-1834). Máquina de tarjetas perforadas. Fue el antecesor de Hollerith.

1ª Generación (1938-1952, 56)

Máquinas basadas en válvulas al vacío. ENIAC (Eckert-Mauchly) primer computador. En 1947 se construyó en la Universidad de Pennsylvania la ENIAC (Electronic Numerical Integrator and Calculator) que fue la primera computadora electrónica. El equipo de diseño lo encabezaron los ingenieros John Mauchly y John Eckert. Esta máquina ocupaba todo un sótano de la Universidad (un cuarto de 6 x 12 mts), tenía más de 18 000 tubos de vacío, 70 mil resistencias, 7500 interruptores, su sistema de trabajo lo constituían 20 registros de 10 dígitos, consumía 200 kW de energía eléctrica y requería todo un sistema de aire acondicionado, pero tenía la capacidad de realizar cinco mil operaciones aritméticas en un segundo.

2ª Generación (1953-1962, 63)

En esta generación las computadoras se reducen de tamaño y son de menor costo. Aparecen muchas compañías y las computadoras eran bastante avanzadas para su época como la serie 5000 de Burroughs y la ATLAS de la Universidad de Manchester. La segunda generación surge cuando se sustituye la válvula al vacío por el transistor. Se corresponde con la aparición de los primeros ordenadores comerciales. Estos ordenadores ya permitían interpretar instrucciones escritas en lenguaje de programación como Cobol o Fortrán.

3ª Generación (1963-1971)

Con los progresos de la electrónica y los avances de la comunicación con las computadoras en la década de los 60, surge la **tercera generación** de las computadoras. Se inaugura con la IBM 360 en abril de 1964. La tercera generación va de 1964 a 1971 y se caracterizó por la utilización del circuito integrado como soporte de la información. Esto permitió abaratar los costos, reducir el tamaño de los ordenadores y aumentar sus prestaciones. Paralelamente se mejoraron los lenguajes de programación y empezaron a aparecer programas comerciales. IBM 360, el primer computador basado en circuitos integrados: 760. Aguantaban 20 terminales y podían encenderse varias veces al día.

Compatibilidad. La IBM, dice a sus clientes que los programas antiguos correrán en los nuevos modelos. Las empresas que compiten con la IBM, recibieron las características estándar, de sus equipos para satisfacer al mercado. PDP-8, PDP-11, de DEC, Modelos de Compatibilidad, supercomputadoras CDC7600 (1969). Ferrita por circuitos integrados para la memoria del computador. Programas que aparecen: Basic y Pascal.

4ª Generación (1972-1987)

Con la aparición del microprocesador que es la integración de todos los elementos básicos del ordenador en un solo circuito integrado surge la cuarta generación. Esta época se caracteriza por la mejora sustancial de los periféricos así como la aparición de lenguajes y herramientas informáticas. Aquí nacen las computadoras personales que han adquirido proporciones enormes y que han influido en la sociedad en general sobre la llamada **“Revolución Informática”**.

En 1976 Steve Wozniak y Steve Jobs inventan la primera microcomputadora de uso masivo y más tarde forman la compañía conocida como la Apple que fue la segunda compañía más grande del mundo, antecedida tan solo por IBM; y esta por su parte es aún de las cinco compañías más grandes del mundo.

En 1981 se vendieron 800 000 computadoras personales, al siguiente año la cifra aumentó a 1 400 000. Entre 1984 y 1987 se vendieron alrededor de 60 millones de computadoras personales, por lo que no quedan dudas que su impacto y penetración han sido enormes.

Con el surgimiento de las computadoras personales, el software y los sistemas que con ellas se manejan han tenido un considerable avance, porque han hecho más interactiva la comunicación con el usuario. Surgen otras aplicaciones como los procesadores de palabra, las hojas electrónicas de cálculo, paquetes gráficos, etc. También las industrias del Software de las computadoras personales crecen con gran rapidez. Gary Kildall y William Gates se dedicaron durante años a la creación de sistemas operativos y métodos para lograr una utilización sencilla de las microcomputadoras (son los creadores de CP/M y de los productos de Microsoft).

Elementos de Arquitectura y Seguridad Informática

No todo son microcomputadoras, por su puesto, las minicomputadoras y los grandes sistemas continúan en desarrollo. De hecho las máquinas pequeñas rebasaban por mucho la capacidad de los grandes sistemas de 10 o 15 años antes, que requerían de instalaciones costosas y especiales, pero sería equivocado suponer que las grandes computadoras han desaparecido; por el contrario, su presencia era ya ineludible en prácticamente todas las esferas de control gubernamental, militar y de la gran industria. Las enormes computadoras de las series CDC, CRAY, Hitachi o IBM por ejemplo, eran capaces de atender a varios cientos de millones de operaciones por segundo.

5ª Generación (1981 - ?)

De 1981 hasta nuestros días se habla de la quinta generación que además de continuar el desmedido avance electrónico, se presta mucha mayor atención al software para acercar el ordenador a la forma de comunicación natural de un sujeto humano. Además en esta época aparece un tipo de ordenador que va a revolucionar el concepto de la informática, el PC (Personal Computer). En vista de la acelerada marcha de la microelectrónica, la sociedad industrial se ha dado a la tarea de poner también a esa altura el desarrollo del software y los sistemas con que se manejan las computadoras.

Surge la competencia internacional por el dominio del mercado de la computación, en la que se perfilan dos líderes que, sin embargo, no han podido alcanzar el nivel que se desea: la capacidad de comunicarse con la computadora en un lenguaje más cotidiano y no a través de códigos o lenguajes de control especializados. Japón lanzó en 1983 el llamado "programa de la quinta generación de computadoras", con los objetivos explícitos de producir máquinas con innovaciones reales en los criterios mencionados. Y en los Estados Unidos ya está en actividad un programa en desarrollo que persigue objetivos semejantes, que pueden resumirse de la siguiente manera:

- Procesamiento en paralelo mediante arquitectura y diseños especiales y circuitos de gran velocidad.
- Manejo de lenguaje natural y sistemas de inteligencia artificial.

El futuro previsible de la computación es muy interesante, y se puede esperar que esta ciencia siga siendo objeto de atención prioritaria de gobiernos y de la sociedad en conjunto.

Clasificación de las Computadoras

1. Supercomputadoras.
2. Macrocomputadoras.
3. Minicomputadoras.

4. Microcomputadoras o PC's.

Supercomputadoras: Una supercomputadora es el tipo de computadora más potente y más rápida que existe en un momento dado. Estas máquinas están diseñadas para procesar enormes cantidades de información en poco tiempo y son dedicadas a una tarea específica. Así mismo, son las más caras, sus precios alcanzan los 30 millones de dólares y más; y cuentan con un control de temperatura especial, esto para disipar el calor que algunos componentes alcanzan a tener. Unos ejemplos de tareas a las que son expuestas las supercomputadoras son los siguientes:

- Búsqueda y estudio de la energía y armas nucleares.
- Búsqueda de yacimientos petrolíferos con grandes bases de datos sísmicos.
- El estudio y predicción de tornados.
- El estudio y predicción del clima de cualquier parte del mundo.
- La elaboración de maquetas y proyectos de la creación de aviones, simuladores de vuelo. Etc.

Debido a su precio, son muy pocas las supercomputadoras que se construyen en un año

Macrocomputadoras: Las macrocomputadoras son también conocidas como Mainframes. Los mainframes son grandes, rápidos y caros sistemas que son capaces de controlar cientos de usuarios simultáneamente, así como cientos de dispositivos de entrada y salida. Los mainframes tienen un costo que va desde 350,000 dólares hasta varios millones de dólares. De alguna forma los mainframes son más poderosos que las supercomputadoras porque soportan más programas simultáneamente. Pero las supercomputadoras pueden ejecutar un sólo programa más rápido que un mainframe. En el pasado, los Mainframes ocupaban cuartos completos o hasta pisos enteros de algún edificio, hoy en día, un Mainframe es parecido a una hilera de archiveros en algún cuarto con piso falso, esto para ocultar los cientos de cables de los periféricos, y su temperatura tiene que estar controlada.

Minicomputadoras: En 1960 surgió la minicomputadora, una versión más pequeña de la Macrocomputadora. Al ser orientada a tareas específicas, no necesitaba de todos los periféricos que necesita un Mainframe, y esto ayudo a reducir el precio y costos de mantenimiento. Las Minicomputadoras, en tamaño y poder de procesamiento, se encuentran entre los mainframes y las estaciones de trabajo. En general, una minicomputadora, es un sistema multiproceso (varios procesos en paralelo) capaz de soportar de 10 hasta 200 usuarios simultáneamente. Actualmente se usan para almacenar grandes bases de datos, automatización industrial y aplicaciones multiusuario. Microcomputadoras o PC's

Microcomputadoras: Las microcomputadoras o Computadoras Personales (PC's) tuvieron su origen con la creación de los microprocesadores. Un microprocesador es "una computadora en un chip", o sea un circuito integrado independiente. Las PC's son computadoras para uso personal y relativamente son baratas y actualmente se encuentran en las oficinas, escuelas y hogares. El término PC se

Elementos de Arquitectura y Seguridad Informática

deriva de que para el año de 1981, IBM, sacó a la venta su modelo "IBM PC", la cual se convirtió en un tipo de computadora ideal para uso "personal", de ahí que el término "PC" se estandarizase y los clones que sacaron posteriormente otras empresas fueron llamados "PC y compatibles", usando procesadores del mismo tipo que las IBM, pero a un costo menor y pudiendo ejecutar el mismo tipo de programas. Existen otros tipos de microcomputadoras, como la Macintosh, que no son compatibles con la IBM, pero que en muchos de los casos se les llaman también "PC's", por ser de uso personal. En la actualidad existen variados tipos en el diseño de PC's: Computadoras personales, con el gabinete tipo minitorre, separado del monitor. Computadoras personales portátiles "Laptop" o "Notebook".

Computadoras personales más comunes, con el gabinete horizontal, separado del monitor. Computadoras personales que están en una sola unidad compacta el monitor y el CPU. Las computadoras "laptops" son aquellas computadoras que están diseñadas para poder ser transportadas de un lugar a otro. Se alimentan por medio de baterías recargables, pesan entre 2 y 5 kilos y la mayoría trae integrado una pantalla de LCD (Liquid Crystal Display). Estaciones de trabajo o Workstations Las estaciones de trabajo se encuentran entre las Minicomputadoras y las macrocomputadoras (por el procesamiento). Las estaciones de trabajo son un tipo de computadoras que se utilizan para aplicaciones que requieran de poder de procesamiento moderado y relativamente capacidades de gráficos de alta calidad. Son usadas para: Aplicaciones de ingeniería CAD (Diseño asistido por computadora) CAM (manufactura asistida por computadora) Publicidad Creación de Software en redes, la palabra "workstation" o "estación de trabajo" se utiliza para referirse a cualquier computadora que está conectada a una red de área local.

Tipos de computadoras

Se clasifican de acuerdo al principio de operación en **Analógicas** y **Digitales**.

Computadora analógica. Aprovechando el hecho de que diferentes fenómenos físicos se describen por relaciones matemáticas similares (v.g. Exponenciales, Logarítmicas, etc.) pueden entregar la solución muy rápidamente. Pero tienen el inconveniente que al cambiar el problema a resolver, hay que realambrear la circuitería (cambiar el Hardware).

Computadora digital. Están basadas en dispositivos biestables, que sólo pueden tomar uno de dos valores posibles: '1' ó '0'. Tienen como ventaja, el poder ejecutar diferentes programas para diferentes problemas, sin tener que la necesidad de modificar físicamente la máquina.

Los ordenadores digitales modernos se apoyan en componentes electrónicos que efectivamente operan como si fueran micro interruptores representando los valores 0 y 1. Estos valores representan la unidad mínima de información con la que puede trabajar un ordenador y se denomina bit (contracción de **binary digit**). Los números binarios son números de base 2. Entonces para medir la capacidad de una

microcomputadora en memoria o espacio físico existen unidades de medidas que se muestran a continuación y que tienen como base el bit:

1 Byte	=	8 bits
1 Word	=	2 byte (16 bits)
1 Párrafo	=	2 word
Segmento	=	64 Kilobyte
1 Kilobyte	=	1024 Bytes
1 Megabyte	=	1 048 576 Bytes
1 Gigabyte	=	1 073 741 824 Bytes

Hay que entender que utilizando esta aritmética binaria un ordenador puede traducir cualquier número que le suministremos, adaptándolo a su forma de funcionar. Las letras del alfabeto y los signos especiales (tales como %, &,\$,!) se representan acudiendo a una nueva unidad de representación mayor, que se obtiene a base de utilizar bloques de bits. Con un número binario de hasta 8 cifras (1 byte - 00000000) se representa desde el 0 hasta el 255. Correspondiendo cada número a un signo o letra a representar tenemos resuelto el problema. El código más extendido en los ordenadores personales es el ASCII (American Standard Code for information Interchange). Los ordenadores operan también con números Hexadecimales base 16 en el que los números decimales del 0 al 9 se usan normalmente y los del 10 al 15 se representan por letras de la A la F. Este sistema se utiliza por razones técnicas con el empaquetamiento de la información.

¿Qué es un microprocesador?

El microprocesador, o simplemente el micro, es el cerebro del ordenador, se encarga de realizar todas las operaciones de cálculo y de controlar lo que pasa en el ordenador recibiendo información y dando órdenes para que los demás elementos trabajen. Es el jefe del equipo y, a diferencia de otros jefes, es el que más trabaja. Es un chip, un tipo de componente electrónico en cuyo interior existen miles (o millones) de elementos llamados transistores, cuya combinación permite realizar el trabajo que tenga encomendado el chip. Los micros, como los llamaremos adelante, suelen tener forma de cuadrado o rectángulo negro, y van o bien sobre un elemento llamado zócalo (socket número en inglés) o soldados en la placa o, en el caso del Pentium II, metidos dentro de una especie de cartucho que se conecta a la placa base (aunque el chip en sí está soldado en el interior de dicho cartucho).

Elementos de Arquitectura y Seguridad Informática

A veces al micro se le denomina "la CPU" (Central Process Unit, Unidad Central de Proceso), aunque este término tiene cierta ambigüedad, pues también puede referirse a toda la caja que contiene la placa base, el micro, las tarjetas y el resto de la circuitería principal del ordenador. La velocidad de un micro se mide en megahercios (MHz), aunque esto es sólo una medida de la fuerza bruta del micro; un micro simple y anticuado a 100 MHz puede ser mucho más lento que uno más complejo y moderno (con más transistores, mejor organizado...) que vaya a "sólo" 50 MHz. Es lo mismo que ocurre con los motores de coche: un motor americano de los años 60 puede tener 5.000 cm³, pero no tiene nada que hacer contra un multiválvula actual de "sólo" 2.000 cm³.

Partes de un microprocesador

En un micro podemos diferenciar diversas partes:

- **El encapsulado:** Es lo que rodea a la oblea de silicio en sí, para darle consistencia, impedir su deterioro (por ejemplo por oxidación con el aire) y permitir el enlace con los conectores externos que lo acoplarán a su zócalo o a la placa base.
- **La memoria caché:** Una memoria ultrarrápida que sirve al micro para tener a mano ciertos datos que previsiblemente serán utilizados en las siguientes operaciones sin tener que acudir a la memoria RAM, reduciendo el tiempo de espera. Es lo que se conoce como caché de primer nivel; es decir, la que está más cerca del micro, tanto que está encapsulada junto a él. Todos los micros tipo Intel desde el 486 tienen esta memoria, también llamada caché interna.
- **El coprocesador matemático:** Más correctamente, la FPU (Floating Point Unit, Unidad de coma Flotante). Parte del micro especializado en esa clase de cálculos matemáticos; también puede estar en el exterior del micro, en otro chip.
- **El resto del micro:** tiene varias partes (unidad de enteros, registros, etc.) que no merece la pena detallar, en este momento.

1a Fase: Era de los microprocesadores (1971-1980)

Evolución histórica – 1ª. Fase

- 1971: 4004, Primer microprocesador (Nov.1971)
- 1974: 8080, 2 MHz, 8 bits, 0.064 MIPS, 6K trans, (Abril 1974).
- 1978: 8086, 5 MHz, 16 bits, 0.33 MIPS, 29K trans, (Junio 1978).
- 1979: 8088, 5 MHz, 8/16 bits, 0.33 MIPS, 29K trans, (Junio 1979)

El 8088 se utiliza en la mayor parte de las máquinas de clase XT. Viene con lo que se acostumbra a llamar paquete de 40 patas DIP (Dual In-line Package). Los 8088 más antiguos son llamados 8088-1, porque solo pueden correr a 6.66, 7.16 u 8

Mhz. El 8088 es el equivalente de aproximadamente 29000 transistores y puede direccionar hasta 1 Mb de Memoria. Tiene una ruta de datos de 8 bits y el tamaño de la palabra es de 16 bits.

Los procesadores de 16 bits son una nueva generación de chips microprocesadores, los cuales, han reemplazado a los microprocesadores de 8 bits y han causado una revolución en el diseño de las microcomputadoras. Las microcomputadoras basadas en los microprocesadores de 16 bits pueden llegar a ser, para ciertas configuraciones y en ciertos cálculos hasta 4000 veces más potentes que las microcomputadoras de 8 bits de los años setenta a un costo relativamente igual.

Ahora ¿Sabía usted que el 8088 salió posteriormente al 8086?

Pues sí, el 8086 era un chip elegante, con una ruta de datos de 16 bits. Pero el lado malo de un micro de 16 bits es que requiere de una tarjeta madre de 16 bits también. Una tarjeta madre 8086 debe contener suficientes circuitos para transportar 16 bits y por lo tanto costar el doble de una tarjeta madre de 8 bits. Además, casi todas las computadoras conocidas en esa época basadas en microprocesador usaban un micro con ruta de datos de 8 bits. Eso colocó a la 8086 en desventaja económica.

Así que para ofrecer el poder del 8086 y conservar bajos precios de las tarjetas madres construyeron el 8088, un año después que salió el 8086. Interiormente, el 8088 es idéntico al 8086. La única diferencia es el tamaño de la ruta de datos que utiliza para transportar los datos que entran y salen del chip. Puesto que es de solo 8 bits de ancho los diseñadores pudieron adaptar fácilmente los diseños existentes al nuevo chip. Como resultado, el 8088 logró cierto éxito en 1979-1981, pero cuando IBM liberó la PC en 1981 basada en el 8088, el éxito moderado se transformó en sorprendente.

2^{da} Fase: Era de las PC (1981-1985)

El 80286 fue un nuevo chip diseñado por Intel en 1981. Está contenido en un cuadro plástico llamado PGA (Pin Grid Array – Disposición reticular de patas). También viene en un paquete más barato llamado PLCC (Plastic Leadless Chip Carrier – Portachip plástico sin soldaduras). El paquete PGA tiene patas a todo su alrededor; el PLCC tiene patas delgadas como de papel de aluminio en su perímetro. El 286 contiene mucho más poder que el 8088. El 80286 es el equivalente de aproximadamente 130 000 transistores en aproximadamente el mismo volumen que los 29 000 transistores del 8088. Debido a esto, el 80286 trabaja más caliente y puede requerir de dispositivos adicionales de enfriamiento. El 286 como comúnmente se le llama alcanza una velocidad máxima de 20 Mhz, tiene una ruta de datos y tamaño de palabra de 16 bits y puede direccionar hasta 16 Mb.

3^{ra} Fase: Era de los 32 bits (1986-200?)

El microprocesador 80386 es un procesador de 32 bits diseñado para soportar aquellos sistemas operativos optimizados para multitarea. Con registros de 32 bits y

Elementos de Arquitectura y Seguridad Informática

caminos de datos, el 80386 soporta direcciones y tipos de datos de 32 bits. El microprocesador 80386 es capaz de direccionar hasta cuatro Gigabyte de memoria física y 64 Tetrabytes, de memoria virtual. La gestión de la memoria integrada y arquitectura de protección incluye registros de traducción de direcciones y mecanismos de protección para soportar sistemas operativos y hardware avanzado de multitarea.

Tipos de datos

La pastilla microprocesadora 80386 soporta varios tipos de datos además de los soportados por el 8086/80286. El microprocesador 80386 soporta enteros con signo y sin signo de 32 bits y campos de bits de 1 a 32 bits de longitud. El microprocesador 80386 soporta los tipos de punteros estándares, definidos para la familia 8086/80286, así como un puntero de desplazamiento de 32 bits y un puntero completo de 48 bits.

El 386 es de 32 bits; el 386 SX es de 32 bits internamente, pero de 16 en el bus externo, lo que le hace hasta un 25% más lento que el original, conocido como DX. El 80386 permite la definición de segmentos de memoria de tamaño variable. Inclusión de una memoria cache interna en el chip.

Su ámbito natural es DOS y Windows 3.x, donde pueden manejar aplicaciones bastante profesionales como:

Ofimática: Microsoft Word, Excel, etc. (versiones para Windows 3.x, de la 1.0 hasta 6.0, según la velocidad y RAM instalada), Lotus SmartSuite (todas las versiones de AmiPro, Lotus 123 para Windows 3.1, etc.), WordPerfect para Windows 3.1 (poco recomendable, es el más exigente en velocidad y memoria). Contabilidad: para DOS o Windows 3.x, muchos programas. Juegos: muy antiguos, aunque numerosos. Internet/E-mail: para los modelos "rápidos" (unos 33 MHz) y con 4 MB RAM, numerosos programas para Windows 3.x.

El microprocesador de 32 bits 80486 ha sido diseñado para soportar aquellos sistemas operativos optimizados para multitareas. Como miembro de la familia 80X86, es totalmente compatible con los procesadores 8086, 80286 y 80386. Este procesador posee un bus de datos dinámico, capaz de soportar tipos de datos de 32 bits, muy similar al 80386. Para elevar su funcionalidad se le ha adicionado:

- Un mecanismo de ráfaga del bus para los llenados a alta velocidad de la cache interna;
- Un mecanismo de invalidación de líneas de la cache;
- Un mecanismo para el control del tamaño de los datos, (8, 16, 32 bits);
- Mejoras en las capacidades de arbitraje del bus y soporte de Paridad.

Su potente bus de direcciones permite direccionar hasta 64 Mbytes de memoria física. Las líneas de dirección son bidireccionales para permitir las invalidaciones de las líneas de la cache. Este compuesto por 30 líneas de dirección (A2-A31) y 4 líneas para habilitar bytes: las líneas de dirección forman los 30 bits más significativos y los pines de habilitación de bytes seleccionan a estos desde una localidad de 4 bytes. El microprocesador 80486 está diseñado para que a 25 Mhz utilice un reloj a 25 Mhz. Esta característica que disminuye el reloj del 80386, permite el diseño de un sistema simple mediante la disminución a la mitad de la frecuencia del reloj requerida en el sistema externo.

Pentium

Con el lanzamiento del P54C, primer miembro de la familia P5, el procesador Pentium (versiones de 60 – 66 Mhz), Intel comienza una nueva etapa en la evolución de los procesadores X86 incorporando novedosas tecnologías en su arquitectura. Es importante resaltar que esta nueva arquitectura de 32 bits define un ancho de bus de E/S de 64 bits aspecto que tiende a la confusión a la hora de definir el tipo de procesador.

Características tecnológicas que definen el rendimiento del Pentium

Diseño Superescalar: Tecnología que permite ejecutar más de una instrucción por ciclo de reloj.

Unidad de Punto Flotante: El nuevo diseño de esta unidad mejora la velocidad de cálculo en software intensivo.

Doble Caché Interna: 8 Kb para datos y 8 Kb para códigos imprimen al CPU mayor velocidad de trabajo al suprimirse tiempos de accesos a la RAM de sistema.

Unidad de Predicción: Consta de un algoritmo que permite seleccionar un conjunto de instrucciones sucesivas para ser ejecutadas de forma más eficiente.

Doble Pipeline: Consiste en una doble vía de entrada de datos y códigos a la Unidad de Ejecución, conocidas como U Pipeline y V Pipeline (ambas de 32 bits).

Versiones disponibles de 100, 120, 133, 150, 166, 200 Mhz (Socket 7)

Pentium MMX

Conocido también como P55C, PP/MT es básicamente un procesador Pentium que incorpora la tecnología MMX de Intel. Esta tecnología incorpora en la microarquitectura del chip un conjunto de 57 instrucciones orientadas fundamentalmente a buscar un mayor rendimiento del procesador en aplicaciones multimedia, así como otras aplicaciones de comunicaciones.

Un ejemplo donde se hace imprescindible el uso de este procesador lo encontramos en aplicaciones que requieran:

Elementos de Arquitectura y Seguridad Informática

- Obtención de imágenes con mayor número de colores.
- Obtención de gráficos más reales.
- Procesamiento de videos en movimiento.

Los procesadores Pentium MMX ejecutan las aplicaciones más comunes entre un 10 a un 20 % más rápido que un Pentium a la misma velocidad, mientras que en aplicaciones propiamente de multimedia alcanza un rendimiento aproximadamente de un 60 % superiores. Versiones disponibles de 166, 200, 233 Mhz. (Socket 7)

Pentium Pro

Primer miembro de la familia P6 de Intel, concebido para desktops de altos desempeños, estaciones de trabajo de ingeniería y servidores de redes. Este procesador incorpora en su arquitectura la tecnología conocida como Ejecución Dinámica, un paso superior de la arquitectura superescalar implementada en los procesadores Pentium. Esta tecnología habilita al procesador para ejecutar instrucciones en paralelo, la misma ofrece la combinación de tres técnicas de procesamiento:

- Predicción de múltiples ramificaciones.
- Predice el flujo del programa a través de varias ramas.
- Análisis del flujo de datos: Organiza las instrucciones para que cuando estén listas sean ejecutadas, independientemente del orden del programa.

Ejecución Especulativa: Incrementa la ejecución del procesador buscando y ejecutando hacia adelante del contador de programa instrucciones que probablemente serán necesitadas por el programa.

Otras características importantes en el diseño de este procesador son:

- Cache L2 dentro del mismo encapsulado del CPU.
- D.B.I (doble Bus Independiente).
- Doble caché L1 (8 Kb dato + 8 Kb código).

Aspectos importantes a destacar que permiten la elevada eficiencia de este procesador son:

- La incorporación de la caché L2 dentro del mismo encapsulado, eliminándose así los inconvenientes asociados los accesos hacia el exterior del CPU.
- La nueva arquitectura D.B.I, esta consiste en asignar un bus particular para la caché L2 independientemente del bus del sistema, resolviéndose así los problemas de embotellamiento que se presentaban el bus de sistema en los procesadores Pentium.

Es importante mencionar que este nuevo bus (bus dedicado para cache L2) trabaja a la misma velocidad del CPU.

Existen versiones disponibles de 166, 180 y 200 Mhz (socket 8)

Pentium II

El incremento de aplicaciones multimedia, el crecimiento explosivo de Internet e Intranet corporativa, la necesidad de manejar grandes volúmenes de datos, impulsan a los fabricantes de procesadores al desarrollo de nuevas tecnologías que impriman a las PC la potencia necesaria para asumir estos retos. El Pentium II, procesador de la familia P6 de Intel con tecnología MMX incorporada sucesor del Pentium Pro.

Este procesador utiliza el novedoso diseño de encapsulado, denominado S.E.C. (Single Edge Contact). Dentro de este cartucho se encuentra la cache L2 y el CPU además de otros componentes electrónicos. Intel ha desarrollado este diseño con vistas a obtener mayor ancho de banda del bus para el futuro, además tener en cuenta técnicas que mejoran la disipación de energía del procesador. Este cartucho utiliza una ranura de conexión conocida como Slot 1 de aquí el nombre comercial Pentium II Slot 1.

El procesador Pentium con tecnología MMX™, ahora disponible con 166 MHz y 200 MHz.

Con tecnología MMX de Intel, las PC's obtienen un nuevo nivel de funcionamiento en multimedia y otras nuevas capacidades que sobrepasan lo experimentado anteriormente.

- Sonido intenso.
- Colores brillantes.
- Rendimiento 3D realístico.
- Animación y vídeo fluido.

Para beneficios de funcionamiento completo, se debe combinar un procesador Pentium con una PC basada en tecnología MMX con programas especialmente diseñados para tecnología MMX.

Características

Con el procesador Pentium II, se obtienen todos los últimos avances de la familia de microprocesadores de Intel: la potencia del procesador Pentium Pro más la riqueza en capacidad de la tecnología mejorada de medios MMX. El procesador Pentium II, entregando el más alto desempeño de Intel, tiene abundante capacidad de desempeño para medios, comunicaciones e Internet en el ámbito empresarial.

Operando a 233 MHz y 266 MHz para desktops y servidores y a 300 MHz para estaciones de trabajo, el procesador utiliza la tecnología de alto desempeño Dual Independent Bus (Bus Dual Independiente) para entregar un amplio ancho de banda

Elementos de Arquitectura y Seguridad Informática

adecuado para su elevado poder de procesamiento. El diseño del cartucho Single Edge Contact (S.E.C) [Contacto de un Solo Canto] incluye 512KB de cache dedicada de nivel dos (L2). El procesador Pentium II también incluye 32KB de cache L1 (16K para datos, 16K para instrucciones), el doble de la del procesador Pentium Pro.

Características Técnicas

Arquitectura Dual Independent Bus (Bus Dual Independiente): al igual que el procesador Pentium Pro, el procesador Pentium II también usa la arquitectura D.I.B. Ésta tecnología de alto desempeño combina ambos, un bus cache L2 dedicado de alta velocidad más un bus del sistema con anticipación que hace posible múltiples transacciones simultáneas.

La tecnología MMX de Intel: la nueva tecnología mejorada de medios de Intel permite al procesador Pentium II ofrecer un alto rendimiento para aplicaciones de medios y comunicaciones.

Ejecución dinámica: el procesador Pentium II usa esta combinación única de técnicas de procesamiento, utilizadas por primera vez en el procesador Pentium Pro, para acelerar el desempeño del software.

Cartucho Single Edge Contact (S.E.C) [Contacto de un Solo Canto]: el nuevo e innovador diseño de empaquetamiento de Intel para éste y los procesadores futuros, el cartucho S.E.C. permite que todas las tecnologías de alto desempeño de los procesadores Pentium II sean entregadas en los sistemas dominantes de hoy en día.

El Procesador Pentium II Trabajando

Diseñado para desktops, estaciones de trabajo y servidores de alto desempeño, la familia de procesadores Pentium II es completamente compatible con las generaciones precedentes de procesadores de Arquitectura Intel.

Las empresas pequeñas tanto como las grandes pueden beneficiarse del procesador Pentium II. Éste entrega el mejor desempeño disponible para las aplicaciones que se ejecutan en sistemas operacionales avanzados tales como Windows 95, Windows NT y UNIX.

Sobre su poder intrínseco como procesador Pentium Pro, el procesador Pentium II aprovecha el software diseñado para la tecnología MMX de Intel para desbordar la pantalla plena, video de movimiento total, colores más vivos, gráficas más rápidas y otras mejoras en los medios. Con el tiempo, muchas aplicaciones para empresas se beneficiarán del desempeño de la tecnología MMX. Éstas incluyen:

- Suites para oficina.
- Lectura óptica de documentos.

- Manejo de imágenes.
- Video conferencia.
- Edición y ejecución de vídeo.

La tecnología MMX mejora la compresión/descompresión de vídeo, manipulación de imágenes, criptografía y el procesamiento I/O - todas estas se usan hoy en día en una variedad de características de las oficinas y medios avanzados, comunicaciones e Internet.

Técnica de la Instrucción Simple, Datos Múltiples (SIMD)

Las aplicaciones de multimedia y comunicaciones de hoy en día con frecuencia usan ciclos repetitivos que, aunque ocupan 10 por ciento o menos del código total de la aplicación, pueden ser responsables hasta por el 90 por ciento del tiempo de ejecución. Un proceso denominado Instrucción Simple Múltiples Datos (SIMD, por sus siglas en inglés) hace posible que una instrucción realice la misma función sobre múltiples datos, en forma semejante a como un sargento de entrenamiento ordena a la totalidad de un pelotón "media vuelta", en lugar de hacerlo soldado a soldado. SIMD permite al chip reducir los ciclos intensos en computación comunes al vídeo, gráfica y animación.

Nuevas Instrucciones

Los ingenieros de Intel también agregaron 57 poderosas instrucciones nuevas, diseñadas específicamente para manipular y procesar datos de vídeo, audio y gráficas más eficientemente. Estas instrucciones están orientadas a las sucesiones supremamente paralelas y repetitivas que con frecuencia se encuentran en las operaciones de multimedia.

Aunque la tecnología MMX del procesador Pentium II es compatible binariamente con la usada en el procesador Pentium con tecnología MMX, también está sinérgicamente combinada con la avanzada tecnología central del procesador Pentium II. Las poderosas instrucciones de la tecnología MMX aprovechan completamente las eficientes técnicas de procesamiento de la Ejecución Dinámica, entregando las mejores capacidades para medios y comunicaciones.

Arquitectura Dual Independent Bus (Bus Dual Independiente)

Para satisfacer las demandas de las aplicaciones y anticipar las necesidades de las generaciones futuras de procesadores, Intel ha desarrollado la arquitectura Dual Independent Bus (Bus Dual Independiente) para resolver las limitaciones en el ancho de banda de la arquitectura de la plataforma actual de la PC.

La arquitectura Dual Independent Bus (Bus Dual Independiente) fue implementada por primera vez en el procesador Pentium Pro y tendrá disponibilidad más amplia

Elementos de Arquitectura y Seguridad Informática

con el procesador Pentium II. Intel creó la arquitectura del bus dual independiente para ayudar al ancho de banda del bus del procesador. Al tener dos buses independientes el procesador Pentium II está habilitado para acceder datos desde cualesquiera de sus buses simultáneamente y en paralelo, en lugar de hacerlo en forma sencilla y secuencial como ocurre en un sistema de bus simple.

Cómo Trabaja

Dos buses conforman la arquitectura Dual Independent Bus (Bus Dual Independiente): el "bus del caché L2" y el "bus del sistema" entre el procesador y la memoria principal.

El procesador Pentium II puede utilizar simultáneamente los dos buses.

La arquitectura Dual Independent Bus (Bus Dual Independiente) permite al caché L2 del procesador Pentium II de 266MHz, por ejemplo, operar al doble de velocidad del caché L2 de los procesadores Pentium. Al aumentar la frecuencia de los procesadores Pentium II futuros, también lo hará la velocidad del caché L2.

El bus del sistema de procesamiento por canalización permite transacciones múltiples simultáneas (en lugar de transacciones únicas secuenciales), acelerando el flujo de la información dentro del sistema y elevando el desempeño total.

Conjuntamente estas mejoras en la arquitectura Dual Independent Bus (Bus Dual Independiente) brindan hasta tres veces el desempeño del ancho de banda sobre un procesador de arquitectura de bus sencillo. Además, la arquitectura Dual Independent Bus (Bus Dual Independiente) soporta la evolución del bus de memoria del sistema actual de 66 MHz a velocidades más elevadas en el futuro. Esta tecnología de bus de alto ancho de banda está diseñada para trabajar concertadamente con el poder de procesamiento de alto desempeño del procesador Pentium II.

Ejecución Dinámica

¿Qué es Ejecución Dinámica?

Utilizada por primera vez en el procesador Pentium Pro, la Ejecución Dinámica es una innovadora combinación de tres técnicas de procesamiento diseñada para ayudar al procesador a manipular los datos más eficientemente. Éstas son la predicción de ramificaciones múltiples, el análisis del flujo de datos y la ejecución especulativa. La ejecución dinámica hace que el procesador sea más eficiente manipulando datos en lugar de sólo procesar una lista de instrucciones.

La forma cómo los programas de software están escritos puede afectar el desempeño de un procesador. Por ejemplo, el desempeño del software será afectado adversamente si con frecuencia se requiere suspender lo que se está haciendo y "saltar" o "ramificarse" a otra parte en el programa. Retardos también pueden ocurrir

cuando el procesador no puede procesar una nueva instrucción hasta completar la instrucción. La ejecución dinámica permite al procesador alterar y predecir el orden de las instrucciones.

La Ejecución Dinámica Consiste de:

Predicción de Ramificaciones Múltiples. Predice el flujo del programa a través de varias ramificaciones: mediante un algoritmo de predicción de ramificaciones múltiples, el procesador puede anticipar los saltos en el flujo de las instrucciones. Éste predice dónde pueden encontrarse las siguientes instrucciones en la memoria con una increíble precisión del 90% o mayor. Esto es posible porque mientras el procesador está buscando y trayendo instrucciones, también busca las instrucciones que están más adelante en el programa. Esta técnica acelera el flujo de trabajo enviado al procesador.

Análisis del Flujo de Datos. Analiza y ordena las instrucciones a ejecutar en una sucesión óptima, independiente del orden original en el programa: mediante el análisis del flujo de datos, el procesador observa las instrucciones de software decodificadas y decide si están listas para ser procesadas o si dependen de otras instrucciones. Entonces el procesador determina la sucesión óptima para el procesamiento y ejecuta las instrucciones en la forma más eficiente.

Ejecución Especulativa

Aumenta la velocidad de ejecución observando adelante del contador del programa y ejecutando las instrucciones que posiblemente van a necesitarse. Cuando el procesador ejecuta las instrucciones (hasta cinco a la vez), lo hace mediante la "ejecución especulativa". Esto aprovecha la capacidad de procesamiento superescalar del procesador Pentium II tanto como es posible para aumentar el desempeño del software. Como las instrucciones del software que se procesan con base en predicción de ramificaciones, los resultados se guardan como "resultados especulativos". Una vez que su estado final puede determinarse, las instrucciones se regresan a su orden propio y formalmente se les asigna un estado de máquina.

Cartucho Single Edge Contact (S.E.C) (Contacto de un Solo Canto)

¿Qué es el cartucho de empaquetamiento S.E.C.?

El cartucho Single Edge Contact (S.E.C) [Contacto de un Solo Canto] es el diseño innovador de empaquetamiento de Intel que permite la entrega de niveles de desempeño aún más altos a los sistemas predominantes.

Utilizando esta tecnología, el núcleo y el caché L2 están totalmente encerrados en un cartucho de plástico y metal. Estos subcomponentes están montados superficialmente a un sustrato en el interior del cartucho para permitir la operación a alta frecuencia. La tecnología del cartucho S.E.C. permite el uso de los BSRAMs de alto desempeño y gran disponibilidad para el caché L2 dedicado, haciendo posible el procesamiento de alto desempeño a los precios predominantes. Esta tecnología

Elementos de Arquitectura y Seguridad Informática

de cartucho también permite al procesador Pentium II usar la misma arquitectura Dual Independent Bus (Bus Dual Independiente) utilizada en el procesador Pentium Pro.

El procesador Pentium II se conecta a una tarjeta madre mediante un conector simple de borde en lugar de hacerlo mediante las patillas múltiples utilizadas en los empaquetamientos PGA existentes. Similarmente, el conector de la ranura 1 reemplaza al zócalo PGA utilizado en los sistemas anteriores. Las versiones futuras del Pentium II también serán compatibles con el conector de la ranura 1.

Aplicaciones del cartucho S.E.C. de Intel

Intel se está moviendo hacia el diseño del cartucho S.E.C. como la solución para los procesadores de alto rendimiento de la siguiente década. El primer cartucho S.E.C. está diseñado para desktops, estaciones de trabajo y servidores de procesamiento sencillo y dual. Posteriormente, Intel optimizará los diseños del cartucho para estaciones de trabajo y servidores de desempeño aún mayor y diseñará soluciones similares, altamente integradas para los sistemas de computación móvil.

Versiones disponibles:

- Klamath 233, 266, 300, 333 Mhz. (66Mhz bus speed)
- Deschutes 350, 400, 450 Mhz (100 Mhz bus speed)

Intel ha lanzado al mercado una versión Pentium II conocido con el nombre Xeon, este no es más que un Pentium II adicionando nuevas características como son:

- Nuevo Socket con mayor números de pines que utiliza Slot 2
- Caché L2 tipo CSRAM (versiones de 512, 1, 2 MB), tendrá la misma velocidad de accesos del procesador, full speed.
- Velocidad del bus a 100 MHz.

El Pentium II Xeon orientado al sector de altas prestaciones requiere de mother board especial, este ultimo debe incluir ranura Slot 2 además de conjunto de chipsets 450NX (hasta 4 procesadores) o 450GX (hasta 2 procesadores).

Celeron

Procesador Celeron es una alternativa Slot1 de Intel enfocada a las necesidades básicas de computación, (aplicaciones de oficina, correo electrónico PC dedicadas a entrada de datos) brindando una plataforma de trabajo similar al Pentium II a un coto inferior. Este procesador está basado en la misma arquitectura de la familia P6 de Intel. Este ha sido el producto mas controvertido de la compañía puesto que en sus primeras versiones no incluye cache L2, limitando así sus prestaciones.

Características del Celeron

- Empaquetamiento tipo SEPP (Single Edge Processor Package), compatible con Slot1.
- Soporta velocidad del bus a 66 Mhz.
- Tecnología MMX de Intel.
- Primeras versiones lanzadas: 266, 300 Mhz (no L2 CACHE)
- Versiones actuales: 300A, 333 Mhz (128 Kb on-die cache L2 full speed)

Intel planea seguir la construcción del Celeron hasta finales de 1999 en tres variantes:

1. Celeron 300a, 333, 366 Slot1 con 128 Kb L2 cache.
2. Celeron en Socket 300A, 333, 366 Mhz con 128 Kb L2 cache (66 Mhz bus speed).
3. Celeron en Socket 300a,333, 366, 400 Mhz con 128 Kb L2 cache (66/100 Mhz bus speed).

Debemos destacar que el futuro Socket de Intel para Celeron de 370 pines no será compatible con la especificación Socket 7.

Pentium III

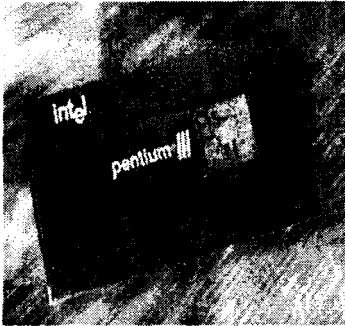
Su lanzamiento fue el 28 de Febrero de 1999 en sus versiones iniciales de 450MHz y 500MHz, y llegará a alcanzar los 750MHz. Cansada de que su competencia (AMD y Cyrix sobre todo) copiara no sólo sus diseños de microprocesadores sino sus mismos nombres comerciales, Intel decidió que el sucesor del 486 no se llamaría 586, sino **Pentium**.

En aquella época parecía imposible que aquel curioso nombre se perpetuara hasta el siglo XXI... pero mientras algunas cosas cambian, como por ejemplo el meritorio paso de AMD de empresa "asimiladora" de ideas ajenas a potente innovadora tecnológica, otras permanecen. Llegó primero el Pentium "clásico", luego el remozado Pentium MMX, el potente e innovador Pentium Pro, el exitoso Pentium II... y ya están ante el Pentium III, también conocido como **Katmai**. ¿Será un digno miembro de la gama Pentium? Veámoslo.

Un vistazo al exterior

A primera vista, un Pentium III (en adelante "**P3**", Figura 1.1) se parece muchísimo a un híbrido de Pentium II y Celeron. Por delante tiene la forma típica de cartucho negro para conectar al Slot1 que ya tenía el Pentium II... pero por el otro lado está desnudo, como el Celeron.

Elementos de Arquitectura y Seguridad Informática



Intel denomina este formato S.E.C.C.2, para diferenciarlo del formato S.E.C.C. del Pentium II y del S.E.P.P del Celeron. El objetivo buscado al eliminar una de las caras de plástico es aumentar la refrigeración de los chips, tanto del micro en sí como de los chips de caché L2, ya que de esta forma el disipador de calor apoya directamente sobre ellos. El nuevo formato es una buena idea, aunque no es algo que emocione demasiado, pero el micro en sí no tiene nada destacable físicamente, se parece mucho a los más recientes Pentium II.

Figura I.1. Vista del Pentium III.

Características técnicas

¿Es innovador el Pentium III? ¿Y si lo es, por qué? Comparémosle con su inmediato predecesor, el Pentium II (Tabla I-1):

Tabla I-1

Características	Pentium II	Pentium III (P3)
Tecnología de fabricación	0,35 y 0,25 micras	0,25 micras
Velocidad	233 a 450 MHz	450 y 500 MHz
Caché L1	32 KB	32 KB
Caché L2	512 KB a la mitad de la velocidad del micro	512 KB a la mitad de la velocidad del micro
Bus de sistema	66 y 100 MHz	100 MHz
Instrucciones especiales	MMX	MMX y SSE
Características especiales		Número de serie individualizado

Bien, parece que no hay muchas diferencias, ¿verdad? Pues no, no las hay. Durante bastante tiempo, muchos esperamos que el P3 llegara al mercado con 64 KB de L1, o un bus de 133 MHz, o con la L2 funcionando a la misma velocidad del micro (como en los Celeron y los AMD K6-3)... vanas esperanzas. Tecnológicamente, el actual P3 es totalmente idéntico a un Pentium II de 350 MHz o más salvo por las nuevas instrucciones SSE.

¿Pentium III = Pentium II MMX-2?

Como decíamos, el salto evolutivo que ha desembocado en el P3 ha sido la incorporación de 70 nuevas instrucciones llamadas oficialmente **SSE, Streaming SIMD Extensions** (extensiones SIMD de flujo), aunque durante mucho tiempo las conocimos como **KNI** (Katmai New Instructions, nuevas instrucciones del Katmai, el nombre técnico del P3) y mucha gente prefiere llamarlas, más comercialmente, **MMX-2**.

Probablemente el nombre más adecuado no sea el oficial, sino el preferido de los publicistas: **MMX-2**. Las originales instrucciones **MMX** significan **MultiMedia eXtensions**, un nombre lógico si tenemos en cuenta que se crearon para aumentar el rendimiento en las aplicaciones multimedia (aquellas que combinan imagen, sonido y/o vídeo). El problema de dichas instrucciones **MMX** (que incorporan todos los micros desde los ya clásicos Pentium **MMX** y **AMD K6**) era que no podían ser utilizadas junto con la **FPU**, la unidad matemática de coma flotante del micro, de enorme importancia en aplicaciones como juegos o **CAD**. Esto hacía que muchos programadores no optimizaran los programas para **MMX**, ya que "sólo **MMX**" o "sólo **FPU**" no era una elección agradable.

El P3 resuelve este problema de dos maneras:

1. Las instrucciones **SSE** permiten realizar cálculos matemáticos con números con coma flotante, al contrario que las **MMX**, que sólo los realizan con números enteros.
2. Las instrucciones **SSE** pueden utilizarse simultáneamente con la **FPU** o con instrucciones **MMX**.

Para entender el proceso que siguen estas instrucciones para acelerar los cálculos podemos fijarnos en la palabra **SIMD**: **Single Instruction, Multiple Data**; instrucción única, datos múltiples. Estas instrucciones permiten realizar una única operación compleja con varios datos en vez de realizar varias operaciones más simples, pudiendo hacer **hasta 4 operaciones en coma flotante** por cada ciclo de reloj.

Además, algunas de estas 70 nuevas instrucciones optimizan el rendimiento en apartados multimedia como la reproducción de vídeo **MPEG-2** o el reconocimiento de voz, mientras otras aceleran el acceso a la memoria.

¿Sus problemas? Claramente, que **para que exista aumento de rendimiento, las aplicaciones deben estar optimizadas para las nuevas instrucciones**. Es decir, que en aplicaciones no optimizadas (el 99,99% de las actuales), un **Pentium II** y un **Pentium III** a la misma velocidad de reloj dan unos resultados idénticos.

Rendimiento: de 0 a 100 (%) en sólo 10 tests

El anterior párrafo terminaba con una afirmación que a muchos les habrá parecido un tanto increíble, después de ver, leer, escuchar y hasta soñar con la "tímida" campaña publicitaria de Intel promocionando el Pentium III. Pues nada, remitámonos a los hechos... o más bien a los números (

Elementos de Arquitectura y Seguridad Informática
Tabla I-2).

Los tests anteriores han sido realizados por la mismísima Intel, así que podemos estar seguros de que son casi objetivos,

Analicemos los resultados según el propósito de cada test:

Ofimática: comprende los test Winstone Business y SYSmark, basados en más de 20 aplicaciones tales como Word, Excel, Lotus 123, WordPerfect, CorelDRAW, Netscape Communicator, etc. En estos dos tests el aumento medio del rendimiento es sólo de un **0,4%**... creo que no hacen falta comentarios.

Sin embargo, en tests optimizados para las instrucciones SSE se alcanza un increíble **73,7%** de mejora; sí, un aumento **increíble**, que debemos poner en su lugar. El "3D Lighting and Transformation Test" es sólo **parte** del mucho más complejo 3D WinBench 99. Si tomamos el resultado del test completo, veríamos que la diferencia es sólo de un **6,2%**.

Tabla I-2

TEST	Pentium II 450 MHz	Pentium III 450 MHz	Incremento de rendimiento
Winstone 99 Business	31,4	31,5	0,3 %
Winstone 99 High End - W. NT 4.0	28,2	28,2	0 %
SYSmark 98	191	192	0,5 %
SYSmark 98 - Windows NT 4.0	204	204	0 %
CPUMark 99	33,5	34,6	3,3 %
WinBench 99 - FPU Winmark	2.280	2.290	0,4 %
MultimediaMark 99 (MPEG/audio)	1.101	1.421	29,1 %
3D WinBench 99 - 3D Lighting & T.	33,1	57,5	73,7 %
Jmark 2.0 - Windows NT 4.0	776	781	0,6 %
SYSmark J	910	922	1,3 %

Fuente: Intel Corporation. Configuración: placa BX, 128 MB PC100, disco SCSI, tarjeta video Diamond Viper V550 AGP 16 MB, 1.024x768x16. Sistema operativo Windows 98 salvo indicación en contra.

Multimedia, 3D y juegos: son el objeto de los tests MultimediaMark, 3D WinBench y FPU Winmark. Como indicábamos en el párrafo anterior, todo dependerá del grado de optimización del programa; si no está optimizado para SSE, no habrá ningún aumento apreciable de rendimiento. Si lo está, veremos un rendimiento entre un 5% y un 25% mayor.

Internet: tiene un test específico, el SYSmark J para medir el rendimiento del micro con código Java, y varios tests que utilizan en parte el Netscape Communicator. En mi modesta opinión, un 1,3% no parece justificar la afirmación de Intel de que con el P3 tendremos "por fin, toda la potencia para vivir Internet a fondo"...

Para terminar tendríamos los **tests sintéticos clásicos**, el CPUmark y el FPU Winmark. El primero mide la "fuerza bruta" del micro en aplicaciones no fuertemente matemáticas ni multimedia (el propio Windows, las de ofimática...) y el segundo la fuerza bruta en operaciones matemáticas de coma flotante (para CAD o juegos no optimizados). Suelen ser tomados como indicativos de lo avanzado de la tecnología interna que emplea el micro, según lo cual un 3,3% y un 0,4% no parecen argumentos suficientes para cambiar de Pentium "II" a "III"... pero yo no entiendo de marketing, claro está.

Coppermine: ¿el auténtico Pentium III?

Ya hemos comentado que el P3, dejando aparte las nuevas instrucciones SSE (que sin duda incrementarán el rendimiento de las aplicaciones que las utilicen), no presenta apenas novedades respecto al Pentium II. Pero no es que Intel no sea capaz de innovar, sino que espera hacerlo con **la segunda versión del P3**, de nombre técnico **Coppermine**. Su nombre no cambiará, seguirá siendo "Pentium III", pero tendrá muchas novedades respecto a los modelos actuales:

- Velocidad de 600 MHz o más;
- Velocidad de bus de 133 MHz;
- Tecnología de fabricación de 0,18 micras;
- 64 KB de caché L1 (probablemente);
- 256 KB de caché L2 integrada, a la misma velocidad que el micro.

De estos avances, el menos significativo es el aumento de la velocidad a 600 MHz. Lo más importante son los cambios en la tecnología de fabricación y las memorias caché; pasar de las 0,25 micras actuales a 0,18 micras hará que el chip consuma y se caliente mucho menos, además de permitir velocidades de unos 800 MHz, algo imposible de alcanzar con la tecnología actual.

Por otra parte, aumentar el tamaño de la caché L1 implica un aumento en torno a un 5 ó 10% en todo tipo de aplicaciones sin necesidad de optimizar, mientras que aumentar la velocidad de la caché L2 resulta igualmente beneficioso pese a reducir su tamaño, como se ha demostrado con el Celeron Mendocino, de rendimiento prácticamente idéntico al Pentium II teniendo sólo la cuarta parte de caché L2. Estos cambios en las caché se notarán especialmente en las aplicaciones ofimáticas, con las cuales el actual P3 no es sino un Pentium II más caro.

Sin embargo, no todo son buenas noticias: para conseguir estos beneficios deberemos utilizar un **nuevo chipset llamado Camino** (tal vez el "440JX"), sucesor de los actuales BX y el primero optimizado para el P3. Así que no lo dude: **deberá cambiar su placa base**, salvo que su actual placa tenga soporte para el nuevo voltaje (¿quizá 1,6 V?) y la nueva velocidad de bus de 133 MHz (esto último no es tan raro, afortunadamente).

Incluso es muy probable que tenga que sustituir la memoria, debido a ese aumento de la velocidad de bus a 133 MHz, excesivo excepto para algunas memorias PC100 de muy alta calidad. Ni siquiera está claro si la nueva memoria será SDRAM de más velocidad (¿PC133?) u otros tipos de memoria como DDR SDRAM, SLDRAM o RDRAM. Intel apuesta fuerte por esta última, por un motivo muy curioso: el diseño es de su propiedad, así que el que quiera usarla debe pagar por ello. Esperemos que los fabricantes, ya un poco hartos (y asustados) de tanto monopolio de Intel consigan ganar esta batalla...

Este procesador no supone una ruptura con la gama Pentium II, como sucedió anteriormente con el Pentium MMX, sino una continuidad, lo cual se aprecia en el hecho de utilizar el mismo encapsulado, la misma cantidad de caché e incluso las mismas placas base (siempre que soporten el bus de 100MHz y actualicemos la BIOS a una versión que soporte este nuevo procesador).

¿Dónde está entonces la gracia? El Pentium III añade 70 nuevas instrucciones MMX (llamadas antes KNI - Katmai New Instructions) diseñadas para mejorar las prestaciones de la unidad de coma flotante del procesador, que al igual que en la tecnología 3DNow! de AMD, permiten ser ejecutadas simultáneamente en paralelo (SIMD - Single Instruction Multiple Data - una sólo instrucción con múltiples datos).

Sin embargo, el modo de ejecución de las nuevas instrucciones es ligeramente diferente del de 3DNow!, por lo que las aplicaciones actuales (mejor dicho, las del futuro inmediato) deben soportar las nuevas instrucciones para sacar provecho de la nueva tecnología aportada por este procesador. Como ya ocurrió con las instrucciones MMX del Pentium, lo más probable es que, salvo alguna honrosa excepción, los juegos serán los que realmente sacarán provecho de las cualidades de este nuevo procesador. De hecho, los primeros juegos en versión Beta que soportan estas instrucciones prometen mejoras de hasta un 25% en velocidad con este procesador.

Como ya ocurrió con 3DNow! y las DirectX6, Microsoft ha anunciado el soporte para estas instrucciones en sus futuras DirectX7 (por algo se empieza).

Las características de este nuevos procesador son las siguientes:

- Velocidades iniciales de 450MHz y 500MHz, esperando llegar a 1 GHz.
- Tecnología de 0'25 micras.
- Bus de 100MHz.
- Voltaje de 2V.
- 70 instrucciones adicionales MMX: 50 nuevas instrucciones para trabajo con coma flotante + 12 instrucciones multimedia + 8 instrucciones para acelerar la RAM.
- 512KB de caché de nivel 2 en el propio procesador funcionando a la mitad de velocidad del procesador.
- Capacidad para ejecutar 4 instrucciones simultáneamente.
- Compatibilidad con la mayoría de las placas Slot 1, con chipset BX o ALI Aladdin Pro, requiriendo la consiguiente actualización de la BIOS.
- Encapsulado SECC2: es como medio encapsulado de Pentium II, con una cara del procesador a la vista, sobre la cual se coloca el disipador.
- Código único de identificación, que tanta polémica ha causado y que parece que se puede ocultar mediante software.

Elementos de Arquitectura y Seguridad Informática

COMPATIBILIDAD: tanto ASUS, como ABIT, como SUPERMICRO ya tienen disponibles actualizaciones de BIOS para sus placas BX que soportan este nuevo procesador, y los demás no tardarán en imitarlos.

PRESTACIONES: Visita en enlace a la primera prueba al fondo de la página, pero puedo anunciarte que son espectaculares, suponiendo un gran avance con respecto a la actual gama Pentium II (según INTEL, además de las nuevas instrucciones, se ha mejorado la arquitectura interna). Cuando existan programas y juegos que soporten las nuevas instrucciones, puede ser la locura.

De todos modos, para poder exprimir a fondo las cualidades de este nuevo procesador, tendremos que esperar al lanzamiento del nuevo chipset de INTEL, el CAMINO i820, con soporte AGP x4, Ultra DMA/66, bus PCI de 66MHz y soporte para las nuevas memorias DDR SDRAM y Direct Rambus DRAM.

Conclusiones

¿Hacen falta conclusiones? Bien, allá van. **¿Es el Pentium III un micro inmaduro? SÍ, SÍ, SÍ. Pero, ¿es un mal micro? NO, NO, NO.** Ambas cosas son ciertas y no excluyentes.

Las nuevas instrucciones SSE (o KNI, SIMD...) son un avance importante, que hará las delicias de los usuarios de juegos y aplicaciones gráficas en general. La idea no es original (AMD la tuvo antes, con sus 3DNow!), pero Intel la ha ejecutado francamente bien; sólo recuerde que **si las aplicaciones no están optimizadas para las nuevas instrucciones, el Pentium III funciona como un Pentium II.**

O tal vez deberíamos decir el actual Pentium III, ya que la combinación Pentium III Coppermine + chipset Camino promete un rendimiento mucho mayor que el actual. Y es que, a mi juicio, **Intel ha sacado al mercado un micro casi "de pruebas"**, al que le faltan muchos avances.

Pentium IV

Ya sabemos cómo se llaman las nuevas tecnologías de las que, en principio, serán el último procesador de 32 bits de Intel, el Pentium 4 o Willamette (Figura 1.2): sus nombres son Netburst y Rapid Execution Engine (REE).

Netburst se refiere a la arquitectura del micro, que **ha sido diseñado casi completamente desde cero**; el hecho de llamarse Pentium 4 es una cuestión de marketing, ya que no se trata de una evolución del diseño de los Pentium (clásico, MMX, Pro, II, III... por no hablar del Celeron). Entre las novedades de esta arquitectura está el **bus de 400 MHz** (¿100 MHz con doble tecnología DDR???) y las **instrucciones SSE2 de 128 bits** (actualmente son de 64 bits).

En cuanto a **Rapid Execution Engine (REE)**, promete mejorar sensiblemente el rendimiento del chip, ya que se refiere a su capacidad para hacer funcionar la

unidad aritmético-lógica de enteros (ALU) al doble de velocidad que el resto del chip.

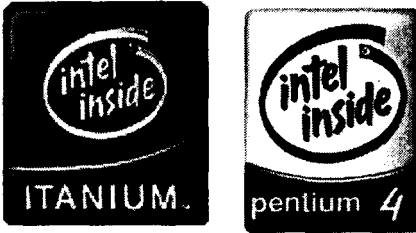


Figura 1.2. Vista de los modelos de microprocesadores Pentium IV

Se ha demostrado ya un prototipo forzado hasta los 2 GHz, sin duda una velocidad mucho mayor a la que se utilizará en su introducción en el mercado. **Los primeros sistemas, basados en memoria Rambus, se esperan para finales de este año.**

El año que viene(2002) saldrán sistemas para memoria SDRAM y/o DDR-SDRAM. El micro utilizará un nuevo conector tipo zócalo, probablemente de 423 pines.

Un portavoz oficial de Intel ha confirmado que se están diseñando chipsets para el próximo Pentium 4 (antes conocido como Willamette) que le permitirán utilizar memoria **SDRAM PC133**. Y no sólo esto, sino que además "se está analizando la opción de crear un chipset para memoria **DDR**" (la DDR es una variante más rápida de la SDRAM).

Esto representa un giro de 180° en la política seguida hasta el momento por Intel con respecto al Pentium 4, que en numerosas ocasiones se aseguró (¿y perjuró?) que utilizaría únicamente memoria RDRAM (Rambus DRAM). Sin embargo, parece que los aún numerosos inconvenientes de esta memoria (y en especial su elevado coste) han inclinado a Intel hacia una solución más pragmática.

La noticia ha afectado seriamente a las volátiles acciones de Rambus, y podría representar un golpe casi definitivo para una tecnología que desde el principio ha tenido numerosos detractores. En todo caso, la cuestión no parece ser tecnológica sino práctica: si la SDRAM y la DDR son fáciles de implementar, baratas y eficaces, y la Rambus es "sólo" eficaz... la elección parece sencilla.

Bien, la noticia oficial se acaba prácticamente aquí, salvo por presentar el nuevo logo (precioso, sin duda alguna) y por recalcar que **será lanzado "en la segunda mitad del año 2000"**. En cuanto a la fecha exacta... ¿?

La velocidad inicial rondará los 1,3 - 1,4 GHz; sigue siendo de 32 bits (no debe confundirse con el profesional Itanium de 64 bits); el bus de sistema será mucho mayor de los 133 MHz actuales (tal vez de 200 MHz, probablemente más); y se supone que utilizará memoria Rambus...

II. Tarjetas principales del sistema en las PC

La Memoria

La Memoria en la computadora es uno de los elementos más importantes e imprescindibles para el buen funcionamiento de esta. Sin duda alguna, la memoria de una PC ha pasado a jugar un papel protagónico en el funcionamiento de la misma, tan importante es conocer la velocidad de la computadora, como la cantidad de memoria que posee.

Allí es donde el Microprocesador de la PC almacena los datos y códigos de los programas. Además, la Memoria es también un canal de comunicación entre el procesador y los periféricos. Por otra parte la estrecha relación que existe entre la velocidad de procesamiento del CPU y la velocidad de respuesta de la memoria puede afectar mucho el buen comportamiento de nuestra computadora. Es algo así como que si el cerebro de un ordenador es el procesador, entonces las memorias pueden ser las neuronas. Los dispositivos de memoria de la PC, lejos de estar concentrados en una única zona se hayan distribuidos por toda ella. Por ejemplo, los registros internos del propio procesador, no son mas que biestables (Dispositivos capaces de almacenar dos estados lógicos). Como su función lo indica son dispositivos almacenadores, en definitiva, elementos de memoria.

La Memoria en una PC se puede clasificar de dos forma: la primera, teniendo en cuenta las funciones generales delimitadas por la tecnología de fabricación y la segunda, el funcionamiento específico que realiza dentro de la PC. Lo cual conduce al surgimiento de áreas dentro de un mismo tipo de memoria

Términos tales como RAM, ROM, Cache o CMOS, pertenecen a la primera clasificación mientras que memoria Convencional, Extendida, Expandida o Virtual se corresponden con la segunda. Estos términos hacen pensar en la complejidad de la organización de la memoria en una PC. Sin embargo, como se podrá ver, cada tipo de memoria desarrolla una función particular y juega un papel muy específico dentro de la arquitectura de la computadora.

En una PC existen por lo general áreas de memoria bien definidas que van más allá de la simple división en memoria RAM y ROM y su utilización depende del tipo de microprocesador empleado y de las necesidades de trabajo. Estas divisiones pueden traer lugar a confusiones en cuanto a su localización, como y quienes pueden usarlas y otras muchas preguntas que frecuentemente nos hacemos ante situaciones donde inexplicablemente nuestra PC, nos informa que no tiene memoria para cargar y ejecutar un programa determinado. La solución más evidente sería colocarle más memoria. Pero antes de actuar tan precipitadamente es mejor revisar como estamos usando la memoria que actualmente tenemos. Ese es precisamente uno de los objetivos de este tema: analizar cada una de estas áreas, determinar su ubicación, como activarlas y por último como usarlas más eficientemente.

De esta forma se pueden identificar seis áreas de memoria bien definidas desde el punto de vista de la función que desempeñan en el sistema:

Memoria convencional.

1. El área reservada del sistema.
2. Memoria Extendida.
3. Memoria Expandida.
4. Shadow RAM.
5. Memoria Virtual.
6. Huecos de Memoria.

y cuatro tipos desde el punto de vista físico o de tecnología empleada en su construcción:

1. Memoria ROM.
2. Memoria DRAM (RAM Dinámica).
3. Memoria SRAM (RAM Estática).
4. Memoria CMOS.

La memoria de un sistema se puede ver como un arreglo de localizaciones con una dirección determinada. Ejemplo, un armario gigantesco con N cantidad de gavetas, cada gaveta posee una etiqueta externa(La dirección) y en el interior encierra un dato determinado. La gaveta posee divisiones internas(Celdas) donde cada una de las cuales guarda un 1 o 0 lógico (Bit). Es decir un arreglo de memoria consiste en N localizaciones, donde cada una almacena un conjunto de bits.

Como podemos observar las direcciones son consecutivas y accediendo a ellas el microprocesador puede leer un dato o escribir un dato. Al nivel de arreglo, la memoria queda representada como muestra la figura II.1 . En esta se observa una memoria típica de 2 a la N localizaciones, constituidas cada una por un conjunto de M celdas que corresponden a una palabra de M bits.

Veamos un acceso común (Figura II.1); su iniciación comienza, cuando la computadora genera una dirección que se corresponde a la localización dada dentro del arreglo. Esta dirección de N bits se almacena en un registro de datos, si se va a leer. Una vez seleccionada la localización esta vierte su contenido en ese mismo registro de datos (Figura II.2).

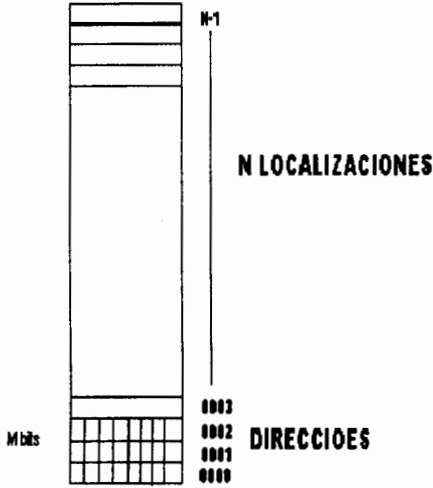


Figura II.1. Esquema del direccionamiento de la memoria.

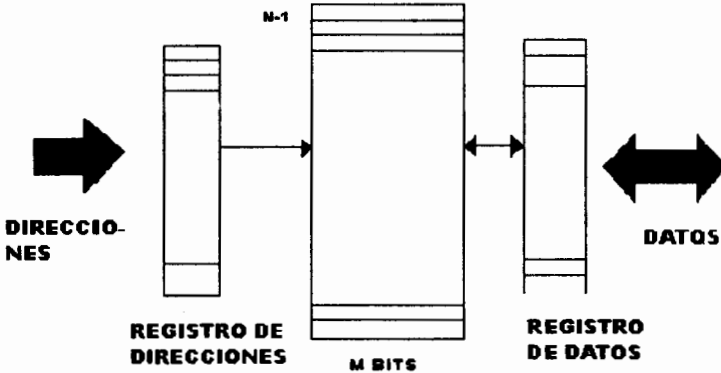


Figura II.2

El subsistema de memoria

Pensemos que tenemos un sistema de 4Mbyte de memoria, distribuidos en 4 módulos de 1Mbyte cada uno, entonces para acceder a una localización de uno de esos módulos se requiere de 2 a la N líneas de direcciones; Donde N es nada menos que 20. Súmele a esto las 16 o 32 líneas de datos, mas señales de control tendríamos como resultado no menos de 50 líneas siendo demasiadas líneas para la implementación del Hardware.

Las computadoras solucionan este problema mediante la técnica de multiplexado. Esta consiste en utilizar las mismas líneas para transmitir en diferentes estados (Figura II.3), diferentes tipos de información. Por ejemplo supongamos que por $N/2$ líneas queremos direccionar un arreglo de 2 a la N localizaciones, pues bien, en un primer paso que llamamos T1 hacemos pasar por las $N/2$ líneas una parte de la dirección que quedara almacenada internamente en el arreglo; En un segundo paso que llamaremos T2 se hace enviar el resto de la dirección.

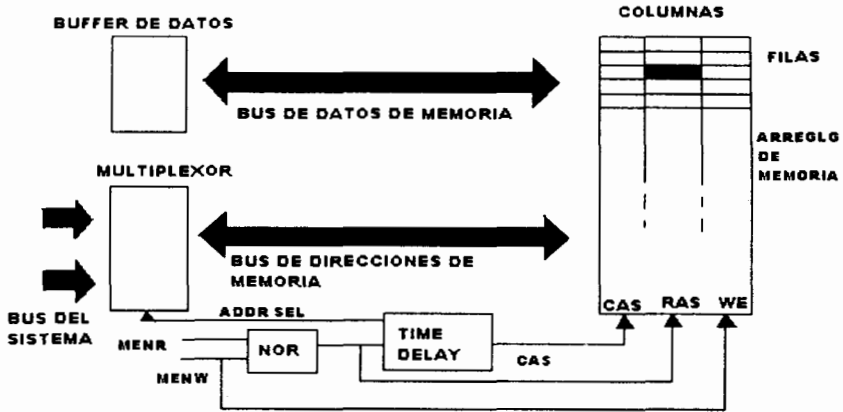


Figura II.3.

Como la localización se selecciona por fila y columna, el multiplexado de direcciones cómodamente separa las dos mitades en dirección de fila y dirección de columna. Los pulsos RAS (Row Address Select) y CAS (Column Address Select) son los encargados de la habilitación de determinada localización en un arreglo de memoria. Como la información correspondiente a cada dirección viaja por las mismas líneas, la generación del RAS y el CAS ocurre en estados diferentes.

Supongamos que se inicia un ciclo hipotético en el subsistema de la figura. Se comienza con las señales MEMR o MEMW (Memory Read o Memory Write), indicativa que se inicia una operación de memoria, ya sea de lectura o de escritura. A partir de una señal como esta, se conforma el pulso de selección de fila, RAS. Es de notar que la dirección de la localización que se va a acceder se coloca en el bus del sistema. Es generada la señal ADDR SEL (Address Selection), que habilita a los bistables que dejarán pasar la primera parte de esa dirección de memoria.

Desplazado en tiempo se genera el CAS, apareciendo este la señal ADDR SEL cambia de estado, permitiendo entonces el paso desde el bus del sistema hasta el de la memoria de la segunda parte de la dirección, seleccionándose la columna y habilitándose la localización en cuestión.

Memorias de solo lectura

Estas son llamadas de solo lectura (Read Only Memory o ROM) porque el Microprocesador no puede escribirla nuevamente, o sea no se puede escribir como la RAM, solo puede leer lo que ya existe en ella, y que guarda la información almacenada en ella incluso después de apagar el equipo. También se puede acceder a este tipo de memoria de forma aleatoria. Se usan generalmente para almacenar datos y códigos de programas que no deben variar, como es por ejemplo el autodiagnóstico que hacen las PC's y el programa que carga el sistema operativo del disco. La configuración de la BIOS de la placa base, así como la configuración de los distintos dispositivos instalados en el equipo se guarda en memoria ROM. A la información de los dispositivos escrita en la memoria ROM de cada uno de ellos se llama FIRMWARE. La ROM estándar se escribe durante el proceso de fabricación de un componente y nunca puede cambiarse.

Según la tecnología empleada en su fabricación se dividen en:

- **ROM** (Read Only Memory).
- **PROM** (Programmable Read Only Memory).
- **EPROM** (Erasable Programmable Read Only Memory).
- **EEPROM** (Electrically Erasable Programmable Read Only Memory).
- **FLASH ROM**.

ROM (Read Only Memory)

La información se pone en el chip en el momento de su fabricación. Se utiliza una Máscara, que es un patrón maestro, para construir varios elementos del circuito sobre el sustrato de Silicio. Este patrón incluye la información que será leída en el dispositivo final.

Este tipo de ROM, ya no es común en las computadoras personales porque ellas requieren que su programación se efectúe durante el proceso de fabricación. Los cambios no son fáciles de hacer y hay que analizar las cantidades que se deben fabricar para hacer la producción rentable.

PROM. (Programmable Read Only Memory)

Este tipo de circuito consiste en un arreglo de elementos que trabajan igual que los fusibles. Las memorias PROM utilizan estos fusibles como elementos de memoria. Normalmente estos fusibles de la PROM conducen electricidad e igualmente que los fusibles normales pueden ser quemados para interrumpir el flujo de la corriente. Todo lo que se necesita es una corriente eléctrica lo suficientemente fuerte para lograrlo, esta corriente es suministrada por un dispositivo llamado Programador de PROM.

Las PROM son fabricadas con todos sus fusibles intactos. Por tanto, puede ser preparada para una aplicación dada usando el programador, el cual destruye los fusibles uno a uno según las necesidades del software que será codificado en su interior.

El efecto de esta programación es permanente, no es posible cambiar o actualizar la información del programa que contiene.

EPROM (Erasable Programmable Read Only Memory)

Es un arreglo de semiconductores. La usan los fabricantes para poder corregir errores de última hora en la ROM. El usuario no puede modificarla. Los datos almacenados aquí pueden ser borrados y el chip puede usarse para otros datos o programas. La programación se realiza utilizando, igualmente, un programador. Este tipo de memoria es fácil de reconocer debido a que ellas tienen una ventana de cristal en el centro de la parte superior de su empaquetadura. Ellas se borran cuando se hace incidir a través de esta ventana una luz ultravioleta de determinada intensidad. Invariablemente esta ventana es cubierta por una etiqueta de algún tipo, para evitar que la información de la memoria se borre accidentalmente. La luz normal de una habitación no provoca este efecto, por que tiene un componente pequeño de luz ultravioleta, no así la luz solar que si puede provocar el borrado de la memoria.

Debido a su versatilidad, memoria permanente y fácil reprogramación este tipo de memoria fue y aún sigue siendo ampliamente utilizado en las computadoras.

EEPROM (Electrically Erasable Programmable Read Only Memory)

Este tipo de circuito en vez de necesitar una fuente muy fuerte de luz ultravioleta, utiliza un voltaje (y corriente) mucho mayor que el normal para borrar su contenido. Este tipo de borrado brinda un importante beneficio: las EEPROM pueden ser borradas y reprogramadas sin sacarlas de sus bases. Las EEPROM brindan a las computadoras y sus periféricos un medio de almacenar los datos sin necesidad de una fuente constante de electricidad. Generalmente utilizadas en aquellas tarjetas que guardan su configuración.

Este tipo de memoria tiene un solo inconveniente y es que tienen limitado el número de veces que pueden ser borradas y reprogramadas (normalmente decenas o cientos de miles de ciclos de borrado-escritura). Al contrario de las memorias RAM en las cuales se puede alterar el contenido de un bit cualquiera, borrar una EEPROM significa eliminar todo su contenido y programar cada bit nuevamente.

FLASH ROM

Es un tipo de EEPROM, que no requiere de voltajes altos ni especiales para borrarlas. Las FLASH ROM pueden ser borradas y reprogramadas utilizando los voltajes normales dentro de la PC, lo cual la hace muy fácil de usar por los diseñadores de estos sistemas. Desdichadamente tienen la misma limitación que las

Elementos de Arquitectura y Seguridad Informática

EEPROM, su vida es finita (aunque mayor que las EEPROM) y (en la mayoría, pero no en todos los casos) deben borrarse y reprogramarse como un bloque. Se usa en la BIOS de los equipos, y de ahí que se llamen FLASH BIOS.

Memoria ROM de Video donde se almacenan los códigos de los caracteres y algunas funciones especiales para el tratamiento de los gráficos. Las tarjetas VGA standard tenían 24 KB de memoria ROM, pero las Super VGA usualmente tienen 32 KB de ROM, Ocupan generalmente las direcciones entre C0000 y C8000.

Localización de la ROM dentro de la PC:

Las memorias ROM se encuentran en la tarjeta madre del sistema y en tarjetas de expansión como tarjetas de video, tarjetas de red, tarjetas controladoras SCSI, etc. Generalmente la memoria ROM se encuentra en un solo módulo de EPROM de 64 Kb. Las direcciones pares e impares residen en el mismo módulo ganando espacio en la tarjeta madre. La más importante es la memoria ROM que contiene al BIOS (Basic Input Output System).

Ocupa la parte alta del espacio de direcciones del primero y el último megabyte (0F0000h y FF0000h) y no es chequeada en ella la paridad. El tiempo de acceso de la EPROM es de 200 ns.. El BIOS es una serie de rutinas básicas de Entrada/Salida agrupadas en la memoria ROM de la tarjeta madre. Ellas suministran al Sistema Operativo el soporte a bajo nivel del Hardware.

Las tarjetas madres tradicionales almacenaban el código del BIOS en memorias EPROM (Erasable Programmable ROM). Si el BIOS necesitaba actualizarse, era necesario quitar esta memoria (usualmente viene en una base), borrarla con luz ultravioleta, reprogramarla y reinsertarla nuevamente en la base.

Áreas de memorias en la PC

Desde el diseño original de la PC, en la década de los 80, la memoria fue uno de los elementos fundamentales en la concepción de las computadoras personales. Los diseñadores se enfrentaban a la necesidad de ubicar en el espacio de direcciones de 1024 KB que permitía el CPU, todos los requerimientos de memoria del sistema. Los procesadores eran de baja velocidad (4.75 Mhz) y no existían mayores dificultades con los tiempos de respuesta de la memoria, Ellos decidieron hacer la siguiente distribución de la memoria:

- 256-640 KB de memoria base o de programa (RAM).
- 64 KB para la ROM BIOS del sistema.
- 128KB para la memoria RAM de la tarjeta de Video.
- El resto de las direcciones de memoria se dejaba disponible para futuras ampliaciones.

Orgullosos de esta solución, nace la primera PC. En un principio nadie podía suponer, ni siquiera imaginar que esta solución con el paso del tiempo - o lo que es lo mismo, con el surgimiento de nuevos y más poderosos procesadores; y con el desarrollo de programas “devoradores” de memoria – quedaría obsoleta y más aún traería nuevas dificultades.

En los sistemas actuales se pueden identificar seis áreas de memoria bien definidas desde el punto de vista de la función que desempeñan en el sistema:

- Memoria convencional.
- El área reservada del sistema.
- Memoria Extendida.
- Memoria Expandida.
- Shadow RAM.
- Memoria Virtual.

En este Capítulo se analizarán cada una de estas áreas; sus características principales; como activarlas, si es necesario y por último como utilizarlas eficientemente para evitar los molestos mensajes de error del sistema.

Memoria convencional

Disponibile en todas las PC. Su capacidad está limitada a 640KB. En ella implícitamente, se cargan los vectores de interrupción, los Controladores de Dispositivos (Device managers), programas residentes (Terminate and Stay Resident, TSR), el DOS y sus aplicaciones. Es accesible por el microprocesador cuando trabaja en modo Real con el sistema DOS o por Windows 95 cuando se selecciona el modo “Solo símbolo del sistema”.

¿Qué es la barrera de los 640K?

Esta barrera no existe físicamente, los programas DOS son casi todos escritos para correr sobre el 8088 (y por supuesto en sus sucesores). Cualquier programa para el 8088 puede direccionar hasta 1024k de memoria (1MB). En teoría, no hay nada en el DOS o en el 8088 que limite este espacio a 640K. Sin embargo, los 640K es una barrera real para la mayoría de los sistemas. ¿Por qué?

El problema de la barrera de los 640K es uno de los problemas más importantes originados por el diseño original de la PC en el año 1980. Donde la memoria de video es compartida por el CPU y la tarjeta de video. El CPU pone aquí los datos para la pantalla y éstos son mostrados en ésta por los circuitos de la tarjeta de video. Por tanto, la memoria de video debe existir siempre y los diseñadores del PC original la pusieron en el rango comprendido entre 640K y 768K, lo cual significa que la mayoría de los programas no pueden usar estas direcciones. Esto se agrava aún más por que los programas necesitan tener bloques de memoria contigua, lo cual no permite que existan “huecos” en la memoria del sistema.

Elementos de Arquitectura y Seguridad Informática

Ud. se puede preguntar: Bueno, ¿por qué no se construye un PC con la memoria de video un poco más alta obteniendo entonces más espacio para memoria convencional?.

Desdichadamente esto no trabajaría, porque existe una gran cantidad de programas que están escritos para manipular directamente la memoria de video y éstos asumen que dicha memoria está en el rango comprendido entre los 640K y los 768K. Además, esto traería como consecuencia la construcción de un PC que no es 100% compatible con los demás y con los programas escritos anteriormente.

El área reservada del sistema

Es el espacio de direcciones de memoria entre 640KB y 1024KB. Es accesible por el microprocesador cuando trabaja en modo Real. En el se encuentran:

Memorias ROM conteniendo software del sistema: ROM BIOS, ROM de video.

Pequeñas cantidades de memoria RAM llamadas buffers o frames usadas por algunas tarjetas de expansión. (Ver I.4.1 ¿Cómo trabaja la memoria LIM?).

128KB separados para la RAM de video.

Zonas de direcciones de memoria no usadas por los anteriores que se pueden dedicar a los Bloques de Memoria Superior, UMB's (Upper Memory Blocks) o para direccionar algunas memorias ROM que se encuentran en tarjetas de expansión.

La memoria ROM BIOS del sistema será tratada posteriormente en este trabajo. Por su importancia trataremos las memorias de la tarjeta de video y los bloques de memoria superior

Memoria sobre la tarjeta controladora de Video.

Como se observa la tarjeta de video tiene incorporada dos tipos de memoria, que tienen funciones diferentes en esta:

Memoria ROM de Video donde se almacenan los códigos de los caracteres y algunas funciones especiales para el tratamiento de los gráficos. Las tarjetas VGA standard tenían 24 KB de memoria ROM, pero las Super VGA usualmente tienen 32 KB de ROM, Ocupan generalmente las direcciones entre C0000 y C8000.

La memoria RAM de video es donde la imagen sobre la pantalla es almacenada en forma digital, con una unidad de memoria asignada a cada elemento de la imagen (ya sea un bit, un byte o algunos bytes). El contenido entero de la memoria es leído de 44 a 75 veces en un segundo mientras se muestra la imagen sobre la pantalla del monitor. Mientras tanto la PC puede tratar de escribir una nueva imagen sobre la memoria.

La siguiente

Tabla II-1 es un resumen de las tarjetas de video más comunes y de sus capacidades de memoria.

Tabla II-1

Tipo de controlador	Espacio de direcciones	Cantidad de RAM (KB)	Cantidad de ROM (KB)
Adaptador de display monocromático (MDA)	B0000-B1000 (4KB)	4	Ninguna en el espacio de direcciones del CPU
Adaptador Gráfico/Color (CGA)	B8000-BC000 (16KB)	16	Ninguna en el espacio de direcciones del CPU
Adaptador de gráficos ampliado (EGA)	A0000-BFFFF (128 KB)	256	C0000-C3FFF (16KB)
Video Graphics Array (VGA).	A0000-BFFFF (128 KB)	256/512	C0000-C5FFF (24KB)
Super Video Graphics Array (SVGA).	A0000-BFFFF (128 KB)	512/1024/2048	C0000-C8000 (32KB)

Tipos de memoria RAM de vídeo

Con chips de memoria DRAM normales, estas operaciones de lectura/escritura no pueden ocurrir simultáneamente. Una debe esperar porque la otra finalice. Esta espera afecta negativamente las prestaciones del vídeo, la velocidad del sistema y su paciencia. Esto se puede evitar usando chips de memoria especial que tienen dos caminos para acceder a cada localización de almacenamiento. A través de uno de ellos el procesador pone la información y a través del otro el sistema de vídeo lo saca

Este tipo de memoria puede existir en dos formas:

Dual-Ported Memory: Memorias de dos puertos que permite escrituras y lecturas simultáneas.

Memoria de Video de acceso aleatorio (Video Random Acces Memory, VRAM), la cual brinda un puerto de acceso completamente de lectura/escritura aleatorio para el procesador, mientras el otro puerto solo permite lecturas secuenciales, lo cual corresponde con las necesidades del rastreo de la imagen del video.

En la actualidad existen otros diferentes tipos de memorias como las EDO RAM y WRAM, aunque estas están siendo sustituidas de forma progresiva por las MDRAM y SGRAM, que trabajan con un ancho de banda de 32, 64 y hasta 128 bits. No obstante, una de las más antiguas (pero que todavía se usa debido a sus excelentes prestaciones) es la VRAM.

Elementos de Arquitectura y Seguridad Informática

La WRAM es también de doble puerto, pero de construcción más avanzada y barata (20% aproximadamente) que las VRAM.

La SGRAM es un tipo de memoria que funcionan en modo síncronico con el reloj del bus, hasta 100 MHz o más. Es una versión de la SDRAM.

Bloques de Memoria Superior. (Upper Memory Blocks, UMB).

Los Bloques de Memoria Superior, también llamados memoria alta del DOS ("High DOS" Memory). Son las áreas que no están dedicadas a memorias ROM y buffers de memoria RAM y que se pueden usar para crear los UMB. Estos no son más que pequeñas áreas de memoria donde podremos colocar los TSR's y los Controladores de Dispositivos con el objetivo de liberar memoria convencional.

Generalmente no toda el área reservada es usada. El área entre 768k y los 960k suman unos 192k. De este espacio un PC típico podría solamente usar 32k de ROM para el video y 64k de PAGE FRAME, si emplea Memoria Expandida; dejando 96k de direcciones sin usar.

Recordemos, por otra parte que la "Limitación de los 640k" no es una verdadera limitación en el modo REAL (Este es el modo en que despiertan los microprocesadores 286 y superiores y en el cual estos trabajan igual que el 8088). La verdadera limitación es 1024KB (ó 1088KB en un microprocesador 286 ó superior). Así el DOS podría usar teóricamente la memoria localizada en el área comprendida desde 768k hasta 960k, si hubiera una forma de poner memoria RAM en esa área y poderla utilizar.

Afortunadamente, esto es posible, si se tiene una computadora con un procesador 386 o superior. Estos procesadores tienen la posibilidad de reacomodar la memoria por software, esto quiere decir que no son necesarios Jumpers o interruptores (Dip Switches) para colocar la memoria dentro de los huecos abiertos entre los 768 K y los 960 K. Para hacer esto Ud. necesita un manipulador de memoria, como el EMM386 suministrado por el DOS.

Veamos cuales son los pasos necesarios para crear y utilizar los UMB:

Identificar las áreas entre los 768 K y los 960 K que no son usadas.

Llenar estas áreas disponibles con memoria (usando un manipulador de memoria), creando los UMB's.

Cargar los TSR's y controladores de dispositivos dentro de los UMB.

1er paso- Identificar el área de memoria disponible

En este primer paso se determinarán las zonas de memoria que no son usadas por ROM o por buffers de RAM. Esto es posible hacerlo usando programas que hagan un análisis de lo que está cargado en memoria y que direcciones de memoria están siendo utilizadas. Programas tan comunes como el Checkit y el MSD.EXE (DOS Ver 6.20) permiten este tipo de operación. En algunos casos también es necesario

consultar la información que se suministra por los fabricantes de tarjetas de expansión para poder determinar que dirección está seleccionada y el rango que ocupa.

2do paso - Crear los UMB's

A través del sistema operativo DOS se pueden crear los UMB's de una forma rápida y segura. Para esto es necesario tener instalados en su disco duro o en su disco de inicio los siguientes ficheros: HIMEM.SYS y el EMM386.EXE, y además, poner los siguientes comandos en su fichero CONFIG.SYS:

```
DEVICE = C:\DOS\HIMEM.SYS
```

```
DEVICE = C:\DOS\EMM386.EXE NOEMS
```

```
DOS = UMB
```

En este ejemplo se está asumiendo que existe un subdirectorio llamado DOS y que en él se encuentran los ficheros antes mencionados. El EMM386 es el encargado de suministrar los UMB's, el parámetro NOEMS provee solo el acceso a los UMB's. Existe el parámetro RAM que puede sustituir a este y que además de permitir el acceso a los UMB's permite la simulación de la memoria expandida en la memoria extendida. Mientras que la instrucción DOS = UMB es la que indica al DOS que puede manipular los UMB's creados por el EMM386.

3er paso- Cargar los TSRs y controladores de dispositivos dentro de los UMB

Para cargar los TSR y controladores de dispositivos dentro de los UMB existen los comandos DEVICEHIGH y LOADHIGH (LH para abreviar) de los ficheros CONFIG.SYS y AUTOEXEC.BAT respectivamente. Esto es válido también para el modo "Solo símbolo del sistema" de Windows 95.

Ejemplos:

```
DEVICEHIGH = C:\DOS\SETVER.EXE (en CONFIG.SYS)
```

```
LH C:\WINDOWS\SMARTDRV.EXE (en AUTOEXEC.BAT)
```

Al ejecutar estos comandos los programas se cargan en memoria de los UMB's con la consiguiente liberación de memoria convencional. Puede resultar interesante correr el comando MEM /C /P antes y después de ejecutar esto para observar los cambios que se producen en la utilización tanto de la memoria convencional como de los UMB's.

En las versiones actuales del DOS (Ver 6.x) existe un programa llamado MEMMAKER.EXE el cual al ejecutarse realiza la optimización de la memoria mediante el movimiento de los TSR's y los Controladores de Dispositivos a la memoria superior. Esto lo hace de la mejor forma posible sin que UD. tenga que revisar la memoria de forma manual y aprovecha al máximo el espacio disponible en la memoria superior. Para usar este programa es necesario tener un microprocesador 386 o superior y memoria extendida. Al concluir la optimización el MEMMAKER le brida un informe de cuanta memoria convencional pudo liberar y

Elementos de Arquitectura y Seguridad Informática

al listar los ficheros del CONFIG.SYS y el AUTOEXEC.BAT verá líneas similares a estas

```
DEVICEHIGH /L:1,12048 =C:\DOS\SETVER.EXE      (en CONFIG.SYS)
```

```
LH /L:0;1,43920 /S C:\WINDOWS\SMARTDRV.EXE  (en AUTOEXEC.BAT)
```

Note que son ligeramente diferentes a los ejemplos anteriores, esto se debe a que MEMMAKER como dijimos anteriormente trata de aprovechar al máximo la memoria disponible en los UMB's. Ud. podrá encontrar más información acerca del MEMMAKER, de los comandos DEVICEHIGH y LH, así como también de sus parámetros, en el HELP que se suministra con la versión 6.0 y superiores del DOS.

Memoria Extendida

La Memoria Extendida es por definición, la memoria que existe por arriba del primer Megabyte de memoria. Debido a esto sólo existe en máquinas basadas en el CPU 80286 y posteriores; no es posible encontrarla en sistemas XT. Tiene además, las siguientes características:

Sólo puede ser usada por un subconjunto de programas DOS, mediante el empleo de manipuladores de memoria como el HIMMEM.SYS del DOS.

Es accesible por el microprocesador solo cuando trabaja en modo protegido. Es ampliamente utilizada por sistemas que trabajan la multitarea como: Windows 3.1, Windows 95, OS/2, UNIX.

Su uso es regulado por la especificación XMS.

XMS Versus Memoria Extendida.

Antes de proseguir hagamos el siguiente experimento, para comprender mejor como funciona la memoria extendida. Despierte su computadora y no permita que se ejecuten los comandos del fichero CONFIG.SYS. Bajo estas condiciones, si se corre el comando MEM/C (DOS ver 5.00 y superior) se observa que los dos últimos mensajes que emite este comando, dicen algo como lo siguiente:

```
9437184 bytes total contiguous extended memory.
```

```
9437184 bytes available contiguous extended memory.
```

Después, reinicie nuevamente y ejecute el CONFIG.SYS con las instrucciones siguientes:

```
DEVICE = C:\DOS\HIMEM.SYS
```

```
DEVICE = C:\DOS\EMM386.EXE NOEMS
```

```
DOS = UMB,HIGH
```

Que cargan el manipulador de memoria extendida HIMEM.SYS y el DOS en el HMA.

Al correr nuevamente el comando MEM/C notaremos que los números y mensajes que corresponden con la memoria extendida son diferentes a los anteriores:

9437184 bytes total contiguos extended memory.

0 bytes available contiguos extended memory.

9371648 bytes available XMS memory.

MS-DOS resident in High Memory Area.

Fíjese que la línea: "contiguos extended memory" es la misma que al principio, pero ahora dice que tiene 0 bytes disponibles de memoria extendida y 9,371,648 bytes libre en la memoria XMS

¿Qué fue lo que pasó?

Primero, note que la diferencia entre el valor total extendido anterior y el total XMS nuevo es exactamente 64K, este es el espacio ocupado por el HMA.

Para comprender mejor la situación de la memoria extendida con respecto a la XMS, hagamos un poco de historia, los primeros programas que intentaban usar la memoria extendida lo hacían a través de dos programas incorporados en el BIOS de la computadora: Move-Block (mover bloque) y Determine-Memory-Size (determine el tamaño de la memoria), conocidos por los programadores como la INT 15, funciones 87 y 88, respectivamente.

La función 88 cuenta la cantidad de memoria extendida del sistema, básicamente mirando dentro del "área total de memoria extendida encontrada", creada por el BIOS cuando la computadora hace el chequeo de memoria.

Un programa podría entonces usar la memoria extendida preparando los datos que él desea mover hacia esta, en un bloque de memoria convencional, entonces lo mueve a una localización de memoria extendida arbitraria con la INT 15, llamando a la función 87 (en lo que sigue lo llamaremos INT 15/87). La INT 15/87 puede también mover datos desde la memoria extendida hacia la memoria convencional. Estos dos comandos eran las bases de programas antiguos como el VDISK.SYS.

El problema con estos programas es que, no hay forma alguna en que la INT 15/87 y la INT 15/88 hagan un chequeo, que asegure que nadie más está usando la memoria: como pueden ser el DOS en el HMA, WINDOWS, etc.

Así es como surgió el XMS, (eXtended Memory Specification). XMS es un conjunto de comandos de programación los cuales, si son seguidos por un programador, obtendrá un programa que puede no solo utilizar la memoria extendida, sino usarla en combinación con otros programas que también la utilicen y sin provocar conflictos de memoria entre ellos.

WINDOWS usa el XMS; Paradox y otros programas son compatibles con XMS. Si Ud. solo corre programas compatibles con el XMS, no habrá problemas. Estos no funcionan como la INT 15, ellos primeros chequean con el manipulador XMS (un programa TSR de cualquier tipo o un Controlador de Dispositivo, en nuestro caso el

Elementos de Arquitectura y Seguridad Informática

HIMEM.SYS) para ver cuanta memoria está disponible y entonces solicitan la memoria que ellos necesitan.

El problema aparece cuando un usuario ejecuta uno de estos programas antiguos. Un programa que utiliza la INT 15 podría ver la existencia de la memoria extendida y usarla, provocando el desplome del sistema. Por esta razón el HIMEM.SYS impide este problema engañando a la INT 15, haciéndole pensar que no hay memoria extendida. Al menos no la memoria extendida que la INT 15 está preparada para usar. Como resultado: los programas antiguos que usan la INT 15 para trabajar con la memoria extendida no corren, porque ellos se encuentran con que no tienen memoria sobre la cual trabajar. Esta es la razón por la cual el comando MEM /P/C informa que existen 0 bytes available contiguous extended memory.

Area de memoria alta. (High Memory Area, HMA)

Existe un pequeño truco en el diseño de los CPU 286 y posteriores. Este consiste en que ellos no solo acceden a 1024K de memoria en modo real (recuerde que el modo real es el modo del procesador sobre el cual trabaja el DOS, y que aquí es donde se emula al 8088). Ellos realmente pueden acceder otros 64K, alcanzando hasta 1088K. Estos 64K adicionales son tomados de la memoria extendida.

No puede cargar cualquier programa dentro del HMA porque en general todos los programas DOS, aplicaciones y utilitarios necesitan cargarse completamente de forma contigua.

A partir del DOS 5.0, este puede realmente depositar la mayor parte de él mismo dentro del HMA, dejando libre mayor cantidad de memoria convencional para aplicaciones normales del DOS. Por supuesto, para obtener los beneficios del HMA, Ud. necesita una computadora con al menos 64K de memoria extendida y con un CPU 286 o superior.

Activando el HMA

Asumiendo que Ud. tiene el hardware apropiado, cargar el DOS (Ver 5.00 y superiores) en el HMA es muy simple, solamente es necesario añadir estas dos líneas a su fichero CONFIG.SYS:

```
DEVICE = C:\DOS\HIMEM.SYS
```

```
DOS = HIGH
```

Ponga la instrucción del HIMEM al principio del archivo CONFIG.SYS, debido a que cualquier otra instrucción que utiliza la memoria extendida debe estar después de esta.

Memoria Expandida

Esta denominación surgió como resultado de las necesidades de memoria de los programas que corrían en las XT. Las compañías LOTUS, INTEL y MICROSOFT colaboraron en un nuevo tipo de tarjeta de memoria, creando un estándar del hardware que permite a los programas DOS acceder a más memoria - 8 Megabytes usando LIM 3.2 y 32 Megabytes usando LIM 4.0.

Este tipo de memoria también se conoce como memoria **LIM** (LOTUS-INTEL-MICROSOFT) o memoria **EMS** (Expanded Memory Specification). Puede ser usada en cualquier tipo de PC, ya sea XT o AT. Es realmente útil bajo DOS con programas que puedan usarla, tales como LOTUS1-2-3 Ver2.X. Computadoras con 386 y posteriores pueden hacer que su memoria Extendida actúe igual que la memoria expandida, también pueden hacerlo algunas máquinas con 286. En la actualidad las nuevas aplicaciones desechan este tipo de memoria, producto de que el procesador puede trabajar directamente con la memoria extendida. No obstante fue muy popular en su época dorada.

¿Cómo trabaja la memoria LIM?

La memoria expandida trabaja usando un sistema de paginado, en el cual existen "páginas" de almacenamiento, disponibles en algún lugar del área reservada entre los 640K y 1024K. Las tarjetas LIM separan 64K de memoria (espacio suficiente para 4 páginas de 16Kb) en el área reservada, esto es lo que se conoce como "Page Frame". LIM puede soportar hasta 2000 de estas páginas (de aquí el tamaño máximo de 32MB) en una tarjeta de memoria que se inserta en los Slots del sistema. Así un programa puede manipular hasta 4 páginas al mismo tiempo en modo real.

Esto trabaja, entonces de la siguiente forma, se trae una página desde la memoria LIM hasta la memoria en el área reservada ("Page Frame"), se escribe y/o modifica y posteriormente se escribe en la memoria LIM. El movimiento de datos entre la LIM y el Page Frame se conoce como paginado.

Cuando un programa como 1-2-3 corre fuera de memoria convencional, él le ordena a la tarjeta de memoria LIM que traiga 4 páginas desde el área LIM y que las ponga en el Page Frame. El puede entonces modificarlo directamente ya que este está dentro del espacio de 1024K de direcciones del 8088 (modo Real). Una vez que estas áreas están llenas, 1-2-3 puede decirle a la tarjeta LIM que devuelva estas páginas al área de memoria LIM, que traiga otras 4 más y así sucesivamente. Este movimiento atrás y adelante, como ya vimos, se llama paginado.

Como es lógico el paginado toma tiempo y, por tanto, la memoria expandida es un poco lenta, pero es mucho más rápida que leer y escribir en disco. Por otra parte recuerde que solo los softwares escritos especialmente para la memoria paginada pueden usar esta memoria.

La memoria LIM es más lenta que la memoria convencional, pero le permite al DOS sobrepasar la limitación de los 640K, con el costo de la velocidad sobre computadoras 8088 y la mayoría de las 80286.

Sobre máquinas 386 y posteriores Ud. puede contar con la compatibilidad de LIM a través de software. Esto es nuevamente posible a través del programa

Elementos de Arquitectura y Seguridad Informática

EMM386.EXE el cual permite simular la memoria expandida sobre la memoria extendida, el crea también el Page Frame en el área reservada y para lograrlo solo son necesarios los siguientes comandos en el CONFIG.SYS:

```
DEVICE=C:\DOS\HIMEM.SYS
```

```
DEVICE=C:\DOS\EMM386.EXE RAM
```

Los cuales deben ser puestos, principalmente lo concerniente al parámetro RAM del EMM386.EXE, si Ud. tiene programas que necesitan la memoria Expandida. Si no Ud. está perdiendo la posibilidad de usar más memoria para los UMB. Existen otros parámetros que permiten regular la cantidad de memoria Extendida que se destinará a Expandida, las direcciones del Page Frame, etc. Para más detalles acerca de los parámetros, uso y posibilidades del EMM386.EXE consulten el HELP del DOS ver 6.0 y superiores.

SHADOW RAM

Los procesadores de 32 y 64 bits pueden acceder a la memoria con transferencias de 8, 16, 32 o 64 bits a través de su bus de datos. Es más conveniente y barato usar un camino de 16 bits o de 8 bits de dato para la memoria ROM BIOS. De esta forma se utilizarían solo dos o un chip de memoria EPROM, en vez de los cuatro requeridos para un camino de 32 bits o de 8 para un camino de 64 bits. Como resultado los accesos a estos chips de memoria se ven penalizados no solo por la lentitud natural del chip sino también porque para leer 32 bits, hay que hacer cuatro lecturas sucesivas y no una como es el caso de la memoria RAM que si cubre todo el tamaño del Bus de datos.

El problema se complica aún más porque algunas de las rutinas del BIOS, particularmente aquellas que usan la tarjeta de video, contienen códigos de programa que se usan con mucha frecuencia (al menos cuando corre MS-DOS).

Para sobreponerse a esta limitante en la velocidad, los fabricantes de computadoras usan la SHADOW RAM. Esto consiste en copiar el contenido de las memorias ROM en la memoria RAM, la cual se lee en palabras de 32 bits. Y ejecutando desde esta los programas que el sistema busca en las ROM. Esto es posible porque se usan las posibilidades del mapeo de paginas de memoria virtual de los microprocesadores iX86, para conmutar el rango de direcciones de la RAM dentro del rango usado por la ROM. Por tanto, la ejecución de las subrutinas del BIOS se verá acelerada en casi cuatro veces.

Esta SHADOW RAM puede habilitarse o no a través de la opción AVANCED SETUP del SETUP del BIOS. Generalmente aparecen unas opciones como estas:

System BIOS Shadow: Enable

Video BIOS Shadow: Enable

C8000-CBFFF Shadow: Disable

CC000-CFFFF Shadow: Disable

D0000-D3FFF Shadow: Disable

D4000-D7FFF Shadow: Disable

Por otra parte, y también con el objetivo de aumentar la velocidad de acceso a las memorias ROM del sistema se pueden cachear también las zonas de memoria correspondientes a la ROM BIOS (F000H – FFFFH) o al BIOS de la tarjeta de vídeo. Esto permite correr estos códigos de programa desde la SRAM en vez de las ROM, o las DRAM (si está habilitada la SHADOW RAM). Para esto es necesario que el controlador de memoria cache esté activado.

Las opciones que permiten cachear los BIOS se encuentran por lo general en CHIPSET FEATURES SETUP y son las siguientes:

System BIOS Cacheable: Enable/Disable.

Video BIOS Cacheable: Enable/Disable.

Algunas consideraciones acerca del uso de la SHADOW RAM

La memoria SHADOW es volátil y debe ser cargada con las rutinas del BIOS, cada vez se despierte la máquina, lo cual puede demorar un poco la carga inicial del sistema.

Se pierde el espacio de RAM que se dedica como SHADOW RAM para otras aplicaciones y este es invisible para el resto del sistema. Por tanto, no se asuste si la cantidad de memoria reportada por el POST es menor que RAM instalada en su PC, esto es muy común si se tiene esta característica habilitada.

En los primeros modelos de PC que brindaron esta facilidad, la relocalización se hacía justo en la frontera de los primeros 16 MB. Esto traía grandes conflictos cuando se quería acceder a memoria más allá de 16 MB. Esto se debía a que la SHADOW RAM (cerca de 256 Kb) interrumpía la continuidad de la memoria RAM y no era posible trabajar con la memoria más allá de los 16 MB. La solución para este problema es muy sencilla, solamente desactive la SHADOW RAM. En las PC actuales el espacio que se dedica a SHADOW RAM se toma desde el tope superior de la Memoria Extendida.

En las computadoras modernas donde se corren Sistemas Operativos como Windows y OS2 se ignoran las subrutinas de video del BIOS y se trabaja directamente con el video. Por lo tanto si trabaja en algunos de estos sistemas operativos desactive la SHADOW RAM por que no esta teniendo un efecto apreciable sobre las prestaciones de su sistema.

También se puede relocalizar las ROM BIOS que estén en ciertas direcciones definidas en el SETUP, algunas veces sin embargo, el código en estas ROM no está diseñado para ser relocalizado y hacer esta operación puede traer como consecuencia que el sistema se bloquee.

Memoria Virtual

Es el espacio físico sobre el disco duro que se usa para el almacenamiento temporal de datos, fundamentalmente por sistemas operativos multitareas como Windows. La memoria virtual permite al sistema operativo liberar RAM para que pueda ser empleada por otras aplicaciones.

Una porción del espacio físico del disco duro se separa para usarlo como memoria virtual. Normalmente este espacio es un fichero oculto al cual se llama fichero de intercambio (Swap File). En Windows 3.X este fichero se llama 386SPART.PAR y en Windows 95 WIN386.SWP.

Este tratamiento de memoria virtual lo permiten los procesadores i386 y superiores mientras trabajan en el modo protegido. Ellos tienen una compleja forma de operación muy parecido al "paginado" de la Memoria Expandida pero con características propias para garantizar la seguridad de la información.

Huecos de Memoria (Memory Hole)

Seguramente este término no es completamente desconocido para los que se han aventurado a explorar un poco las opciones del BIOS, pero su sola presencia no nos da siquiera idea de que se trata; aunque se habilite o deshabilite en el SETUP no notamos ningún cambio apreciable. Pero cuidado, si tiene más de 16 MB podrá encontrar una sorpresa desagradable cuando habilite esta opción.

Los Huecos o Apertura de la memoria no son más que un determinado rango de direcciones de memoria que usan ciertos dispositivos para operaciones de entrada / salida, usando mapeo de memoria. Es decir, la PC envía y recibe señales de dato y control hacia y desde un dispositivo a través de un determinado rango de direcciones. Uno de los dispositivos más comunes que usa este tipo de direccionamiento de memoria son algunas tarjetas de vídeo como la XGA, introducidas por IBM en 1991.

Hasta esta fecha, la mayoría de los adaptadores de vídeo seguían el estándar de la VGA para direccionar la memoria, es decir, la conmutación de bancos dentro del marco de 64 KB que existe en el área reservada del modo real. Esta conmutación de bancos complica la programación del software gráfico y demora la velocidad del vídeo. La XGA de IBM adicionó un modo de direccionamiento que escribe en la memoria directamente, lo que significa que existe un rango de direcciones en la memoria extendida para direccionar directamente el buffer de memoria de la XGA.

Debido a que los adaptadores de vídeo, tienen su propia memoria, ellos no roban la RAM instalada en el PC. Por tanto debido a que este buffer de memoria no es usado por los programas en ejecución, no es necesario que él esté contiguo con el resto de la RAM. En teoría no debe existir ningún problema.

Con los buses de expansión avanzados que pueden direccionar 4 GB completos, casi nunca esto es un problema. Como muchas direcciones están disponibles, no hay oportunidad de conflicto. Pero con el viejo bus ISA, la apertura de memoria restringe severamente la expansión de la memoria RAM. Debido a que los adaptadores de video deben estar en un Slot y como el bus ISA, está limitado a 16 MB, la apertura de memoria usada por el adaptador de video debe aparecer por debajo de la frontera de los 16MB. La memoria por arriba de la apertura de los 16 Mb no puede, por tanto, ser alcanzadas por ningún sistema operativo, debido a la interrupción que se produce en la continuidad de la memoria.

La apertura propiamente “roba” un Mbyte o dos, así que Ud. se quedaría con una PC que le brinda 14 MB de memoria máximo, no importa cuanta RAM Ud. tenga instalada

Este límite de la apertura usualmente no ocurre con los buses Microcanal, VL-BUS, EISA o PCI ya que los cuatro permiten un direccionamiento de 32 Bits y no fuerzan a que la apertura esté por debajo de la frontera de los 16 MB.

En los BIOS modernos en el CHIPSET FEATURES SETUP existe la opción “Memory Hole at 16 MB”, esta opción suele tener dos valores: Deshabilitada (Disable) o Habilitada (Enable, o 15-16MB). Esta opción está diseñada para algunos sistemas operativos con tarjetas de expansión especiales las cuales necesitan el espacio de memoria entre los 15 y 16 MB, si no tiene alguna de estas tarjetas desabilite esta opción.

El seleccionar “15-16 MB” significa que cuando la memoria del sistema es igual o mayor que 16 MB, las direcciones físicas del CPU correspondiente a este espacio de memoria se relocalizarán en el espacio de direcciones correspondiente al bus ISA y habrá un “hueco” de 1 MB en la memoria. Por tanto, bajo el ambiente DOS y Windows, el tamaño de la memoria base es de 640 KB y el de la extendida es de 14 MB. Estos sistemas podrán usar solamente 15 MB aún cuando el sistema tenga instalado más de 16 MB.

Este tipo de direccionamiento no se debe confundir con el método que emplean ciertas tarjetas madres que traen el controlador de video integrado y que usan parte de la memoria RAM del sistema como memoria de Video. El tamaño de la RAM de Video se selecciona por el BIOS y puede llegar hasta 4 MB.

En este caso la memoria de video se toma a partir del límite superior del total de la memoria RAM instalada, lo cual no produce el “hueco” o discontinuidad en la memoria, pero si la disminución de esta en la cantidad que seleccione como memoria de video. En la tarjeta madre ASUS SP97-V existen dos opciones en el CHIPSET FEATURES SETUP que permiten seleccionar el tamaño de esta memoria y la velocidad del reloj que utiliza la tarjeta de video.

Onboard VGA Memory Size	1/2/4 MB
Onboard VGA Memory Clock	Fast/Fastest/Normal

Proceso de arranque

Secuencia de arranque de una PC

Como se observo el BIOS de sistema es el programa que se corre cuando usted energiza la PC. La secuencia de los pasos de dicho programa son en general similares si bien varia del tipo de fabricante que diseña el BIOS, muy ligado al tipo de tarjeta madre y finalmente a los periféricos que usted tienen enganchado a la PC. Dichos pasos se pudieran resumir:

La alimentación de la fuente llega a la tarjeta madre y con ella al sistema completo. Es de destacar que las fuentes de alimentación demoran un tiempo en generar voltajes estables y dentro de los parámetros de operación permisibles, por lo que típicamente se valen de una señal llamada Power Good indicándole a los circuitos lógicos asociados al procesador central que de un reset al mismo para iniciar su operación.

Cuando el procesador sale del modo reset el mismo inicia una búsqueda de instrucciones en una dirección alta de memoria, típicamente los últimos 16 bytes del arreglo de memoria ROM. Los fabricantes obligan al procesador a iniciar su ciclo de trabajo en esa zona con vistas a compatibilizar el trabajo de la PC y permitir que el programa almacenado en la ROM pueda variar de tamaño. En esa zona lo único que se coloca es un "salto" instruyendo al procesador a ir a la dirección de inicio del programa BIOS.

La primera subrutina grabada en el BIOS de una PC recibe el nombre de POST que viene del ingles Power On Self Test (o test de autochequeo). El mismo no es mas que un conjunto de instrucciones que posibilitan la *inicialización, programación* y chequeo de todos los subconjuntos que componen una PC, como lo son los controladores de DMA, de interrupciones, de memoria, etc. Si el POST encuentra un error automáticamente detiene el proceso. En ocasiones brindando un código de error que se traduce en una secuencia de 0 y 1 por algunos puertos específicos o/ y un conjunto de beeps por la bocina. Los técnicos de computadoras utilizan dichos códigos para diagnosticar posibles fallas en la circuitería de la tarjeta madre.

Una vez concluido el POST el BIOS busca la presencia de la tarjeta de vídeo, busca el programa propio que esta tiene grabada en su ROM y le cede el control temporalmente. Este a su vez *inicializa la tarjeta de vídeo* y es entonces cuando por primera vez aparece información en la pantalla del monitor. Aunque muchas veces fugazmente el fabricante de la tarjeta de vídeo informa de la marca de la misma, cantidad de memoria y versión del BIOS almacenado en ella.

Luego, retomando el control el BIOS de la PC busca por la presencia de otros dispositivos en la computadora que requieran de programas específicos de inicialización. Por ejemplo los discos duros IDE/ATA ubican el programa de iniciación del disco de manera general en la dirección C8000h.

El BIOS "imprime" en pantalla la información sobre su versión, fabricante, etc.

Elementos de Arquitectura y Seguridad Informática

El programa inicia chequeos más generales del sistema, como lo es el conteo completo de la memoria. En caso de encontrar algún error este generará en pantalla el correspondiente mensaje.

Acto seguido se realiza un inventario total del sistema, donde se inspecciona que tipo de hardware lleva la computadora. Los BIOS modernos poseen muchos parámetros que configuran de manera automática como lo son las cartas de tiempo de los accesos a memoria, los parámetros de los discos duros, características de los puertos de entrada / salida, COM y LPT, tipo de procesador, etc.

Si el BIOS es PNP compatible, detectara, inicializara y configurara los dispositivos con esta característica, mostrando en pantalla los mensajes correspondientes.

Generación de un sumario de la configuración de su PC. Este es útil para conocer que recursos posee disponibles y si alguno de ellos falló o no está presente. Desgraciadamente esta información es barrida en un abrir y cerrar de ojos.

Finalmente el BIOS pasa el control al dispositivo de booteo. Los BIOS modernos permiten escoger cual es el dispositivo que iniciara el boot del sistema, ya sea el floppy (ya hoy poco probable), el disco duro o el CDROM. Si el BIOS no encuentra a quien ceder el control del boot generalmente se detiene, mostrando el mensaje correspondiente.

Si una máquina llega a este punto, significa que se puede cargar cualquier sistema operativo y, por consiguiente, las utilerías que consideremos convenientes para la tarea de diagnóstico y corrección. Si en alguno de los pasos de la rutina POST, el BIOS detectara algún mal funcionamiento, esto significaría que la operación de todo el sistema no sería confiable. Por lo tanto, para evitar que el usuario utilice una máquina que probablemente le proporcione resultados erróneos, los diseñadores decidieron que cuando la POST detectara alguna falla, toda la máquina se bloqueara, impidiendo la continuación del proceso de arranque y, obviamente, imposibilitando la carga del sistema operativo o de cualquier otro programa.

Pero entonces, ¿si no se puede usar ninguna utilería para determinar la causa del desperfecto, ¿Cómo saber por donde comenzar la tarea de reparación?

Los códigos POST

Cuando comenzaron a salir las primeras máquinas AT, la estructura de las computadoras personales creció en complejidad, de modo que ya no resultaba tan sencillo como antes localizar algún componente defectuoso en la estructura de la tarjeta madre o entre sus periféricos esenciales.

En vista de esta complejidad, para facilitar la labor de detección y corrección de problemas en sus computadoras, los diseñadores de IBM incluyeron una serie de "banderas" al inicio de cada una de las pruebas realizadas durante el encendido de la máquina

Estas "banderas" se enviaron en forma de una palabra de 8bits hacia el puerto 80H de los slots de expansión. Con ellas, si el BIOS iba a verificar el funcionamiento de la memoria RAM, antes de hacerlo expedía un aviso indicando que se iba a realizar ese análisis, de modo que si la prueba fallaba, el técnico tenía un punto de referencia para iniciar la reparación del sistema.

Además, con una tarjeta especial para obtener y desplegar dichas "banderas", el especialista podía verificar en cuál de los códigos el sistema se bloqueaba, consultar en una serie de tablas qué significaba dicho código tomando en cuenta el modelo de la computadora y con la información obtenida iniciar el aislamiento y corrección del problema.

Este método facilitó la tarea de diagnóstico en las plantas de ensamble de computadoras y pronto fue emulado por otros fabricantes, aunque algunos de ellos introdujeron variantes para evitar en lo posible problemas con patentes. Así, encontramos que las máquinas Compaq generan sus códigos POST al igual que las IBM, pero en vez de enviarlos a la dirección 80H, los direccionan hacia la 84H; esto significa que una tarjeta de diagnóstico dedicada exclusivamente a leer los códigos POST de máquinas IBM no servirá en sistemas Compaq y viceversa.

Cabe aclarar que en un principio IBM mantuvo en secreto los códigos POST, así que algunos fabricantes de clones de AT produjeron sus computadoras sin tener idea de esta nueva prestación, por lo que se vendieron una gran cantidad de máquinas de la segunda generación que no los contenían (las máquinas que aún carecen de Setup, tampoco generan estos códigos).

¿Qué es una tarjeta POST?

Dado que las banderas se generan sólo dentro de la tarjeta madre y no se expiden en la pantalla o en la impresora de la unidad; es necesario un dispositivo de captura digital para que recoja estas señales del bus de expansión, sin tener que recurrir a instrumentos complejos, permitiendo así al técnico de servicio visualizar estos códigos y aprovecharlos en su labor. Inicialmente, considerando que en un momento dado no se contara con prácticamente ninguna herramienta especializada para realizar un diagnóstico, algunos fabricantes decidieron que sus códigos POST se expidieran utilizando un medio sobre el cual el CPU tiene control prácticamente desde el inicio: el altavoz interno que se incluye en toda PC.

Con este método, cuando un sistema no enciende correctamente (no alcanza a cargar el sistema operativo), un técnico experimentado puede determinar la causa del problema o al menos tener una aproximación muy cercana, con sólo escuchar el código de beeps que produce la máquina.

Ahora bien, debido a que la rutina POST revisa secuencialmente una gran cantidad de elementos, los fabricantes codificaron cuidadosamente la secuencia de beeps que se expiden en cada caso, de modo que el profesional de servicio reconozca fácilmente en cuál de las pruebas se ha detenido el proceso de arranque. Por ejemplo, hay fabricantes que en caso de que falle el teclado, determinan que el

Elementos de Arquitectura y Seguridad Informática

altavoz suena tres veces; si lo que falla es la tarjeta de vídeo sonará cinco veces; si es una falla en puertos pitará siete veces, etc.

Pese a todo, esta aproximación ofrece muy pocas opciones a los fabricantes para representar la gran cantidad de elementos que se revisan en cada arranque de la PC; así que otros productores decidieron hacer una combinación, de beeps largos y cortos, con lo que por ejemplo, combinando 5 beeps, se pueden representar hasta 32 mensajes de error diferentes.

Si bien, esta aproximación le dio más flexibilidad al despliegue de los códigos POST auditivos, aún eran insuficientes para representar las varias docenas de pruebas que realiza dicha rutina durante el encendido de una computadora típica (además, este método se presta fácilmente a errores, ya que el técnico encargado de la reparación, puede confundir un beep largo con uno corto o viceversa). A la fecha, algunos fabricantes de tarjetas madre aún utilizan el método de los códigos sonoros, así que es necesario familiarizarse con el sonido que produce cada máquina durante el encendido.

Si bien el método de los códigos audibles resultó eficiente, no se podía asignar una combinación de sonidos a todas y cada una de las pruebas realizadas durante la rutina POST, debido a que los elementos a revisar son docenas si no es que cientos.

Por tal razón, para complementar al código sonoro, IBM hizo que el BIOS expidiera a través de la dirección 80H de los buses de expansión, una palabra de 8 bits representando al elemento específico que se fuera a probar a continuación (8 bits permitiría representar hasta 256 elementos diferentes).

Para poder visualizar de forma sencilla estos códigos, es necesario colocar en cualquiera de las ranuras de expansión una tarjeta de diagnóstico cuya función exclusiva es recoger los datos enviados a la dirección 80H durante el encendido y mostrarlos en forma de números hexadecimales. De esta manera, el técnico, tras consultar una serie de tablas donde se consigna qué número corresponde a qué prueba, puede identificar de forma rápida y sencilla el elemento problemático. Así fue como se incorporó el uso de la tarjeta POST.

El BIOS

El término BIOS significa Sistema Básico de Entrada-Salida (Basic Input/Output System). Consiste en el software mínimo e imprescindible que necesita el hardware del ordenador para iniciar e interactuar con el sistema operativo al nivel más bajo, es decir consiste en una serie de subrutinas básicas de Entrada/Salida, de ahí su nombre, agrupadas en la memoria ROM de la tarjeta madre. Ellas suministran al Sistema Operativo el soporte a bajo nivel del Hardware. Esto significa que es el BIOS el que interactúa directamente con el Hardware. Este software y los parámetros que configuran su comportamiento se almacenan en la CMOS, una RAM de 64 o más bytes de capacidad, que se alimenta de una pequeña pila

(níquel-cadmio o lítico). Las memorias ROM se encuentran en la tarjeta madre del sistema y en tarjetas de expansión como tarjetas de vídeo, tarjetas de red, tarjetas controladoras SCSI, etc. Una de las más importante es la memoria ROM que contiene al BIOS. Ocupa las direcciones de memoria desde E000: 0000 hasta F000:FFFF. Las tarjetas madres tradicionales almacenaban el código del BIOS en memorias EPROM (Erasable Programmable ROM). Si el BIOS necesitaba actualizarse, era necesario quitar esta memoria (usualmente viene en una base), borrarla con luz ultravioleta, reprogramarla y reinsertarla nuevamente en la base. En la actualidad la mayoría de las tarjetas madres presentan el BIOS en memorias Flash ROM, la cual para su actualización solo necesita un programa utilitario para programarla, sin necesidad de abrir la máquina ni cambiar físicamente el circuito integrado de memoria que contiene la ROM BIOS. Este programa utilitario, así como los ficheros que contienen el código del BIOS a actualizar y el procedimiento que se debe seguir para la actualización se encuentran por lo general en las páginas WEB de los fabricantes de tarjetas madres más importantes (ASUS, FIC, AOpen, etc.)

Mediante estas actualizaciones se logran eliminar errores en el programa del BIOS y sobre todo añadir nuevas normas y opciones. Como por ejemplo los modos de transferencia UltraDMA, soporte de nuevos modos de ahorro de energía o cualquier norma nueva que saliera y que pudiera soportar el Hardware de la tarjeta madre y que el BIOS original no lo permita.

La operación de actualización del BIOS es un proceso muy sencillo y rápido de ejecutar. Aunque eso sí, tiene su riesgo. La actualización consiste en ejecutar un pequeño programa que tras preguntarnos si queremos actualizar el BIOS hará una copia del actual para, acto seguido, actualizar los datos en la Flash ROM. Si quisiéramos recuperar el antiguo contenido, sólo tendremos que repetir el proceso de actualización con los datos guardados anteriormente. Hay que tener presente que, una vez comenzado el proceso de actualización, **no puede ser interrumpido por ningún motivo**. Si esto sucediera el BIOS no tendría información correcta y la tarjeta madre pudiera no arrancar.

El tamaño de la memoria ROM para almacenar el BIOS, se ha incrementado de 64KB, en las primeras XT, hasta 128KB, debido al incremento de las nuevas funciones que realizan estas rutinas. Aunque es común encontrar algunas tarjetas con memorias de 1024KB Flash ROM y hasta de 2048 en sistemas Pentium II.

Normalmente existen Jumpers que permiten seleccionar el voltaje de alimentación de estas memorias Flash ROM (5V o 12V). Generalmente este voltaje viene bien seleccionado desde la fábrica y no es necesario modificarlo. Una mala selección podría dañar seriamente la pastilla y provocaría que la tarjeta madre no funcionara.

Contenido de una memoria Flash ROM de 1024 KB

La figura 1 muestra la distribución que hace AWARD del contenido de la memoria Flash ROM. Note que existe una distribución original compactada, que es lo que está realmente almacenado en el Chip de memoria Flash ROM y otra descompactada sobre la RAM del sistema (Shadow RAM). Analicemos cada uno de sus elementos por separado.

BIOS compactado (Flash ROM)

Bloque de carga (Boot Block), contiene los primeros 8KB de código que se ejecutarán después de encendida la máquina.

PnP (ESCD), zona de 4KB donde se almacenan la configuración del Hardware Plug & Play. La especificación PnP sugiere la interface estándar para esta zona, la cual puede ser actualizada por el BIOS y por sistemas Operativos PnP, como Windows 95, para configurar los recursos del sistema y prevenir conflictos. Si es observador habrá notado el siguiente mensaje, "Updating ESCD...", cuando reinicia la máquina después de hacer algún cambio en la configuración del hardware o poner algún elemento nuevo.

DMI, zona de 4 KB, es opcional y depende de si se usa un Utilitario de Configuración **DMI** (Desktop Management Interface). En estos 4 KB se almacenan al nivel de BIOS una base de datos de la configuración del sistema conocida como **Management Information Format Database (MIFD)**. El BIOS es capaz de determinar y grabar en esta zona, información pertinente al sistema, tales como: Tipo y Velocidad del CPU, Frecuencia Interna/Externa y tamaño de la memoria, etc. A través de un sistema **DMI** se pueden obtener y modificar en tiempo real los datos de esta base de datos. Este utiliza la misma tecnología empleada para el PnP lo cual permite una actualización dinámica en tiempo real de la información del **DMI**, sin necesidad de crear un fichero imagen del BIOS y actualizar todo su contenido.

Además el Utilitario **DMI** permite al usuario final adicionar a la **MIFD** información que el BIOS no es capaz de detectar como pueden ser los números de serie, información del vendedor y otros datos de interés.

Código de descompactación. La función principal de este bloque es determinar el tamaño de la memoria, crear la Shadow RAM y descompactar en la memoria RAM el código del POST, el SETUP y las rutinas de Entrada/Salida del BIOS (

Figura II.4).

BIOS VGA y SCSI

64 KB de código compactado de BIOS.

BIOS descompactado (Shadow RAM).

8 KB de código de BIOS compatible IBM.

24 KB de código de rutinas de E/S.

32 KB de código del Programa SETUP.

64 KB de código del POST. Antes de cargar el sistema existen aquí los 64 KB correspondiente al código del POST. Después de la carga del sistema están vacíos.

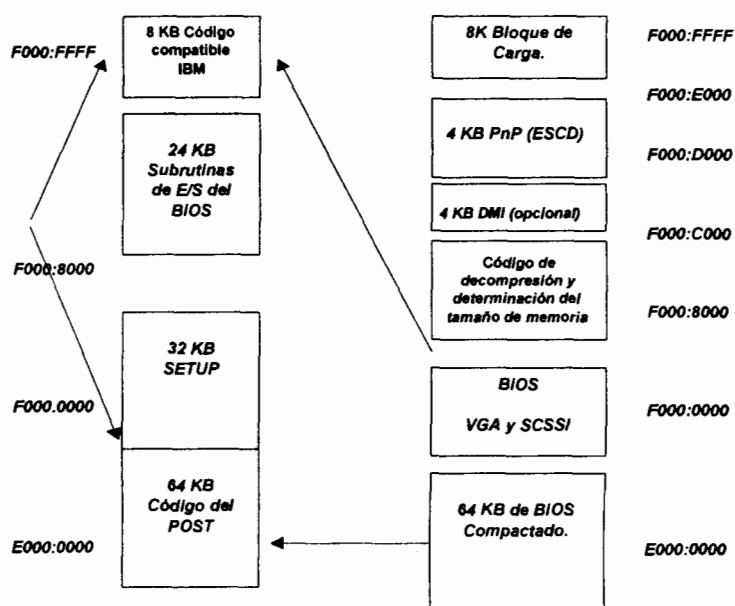


Figura 11.4. Distribución de contenido de la memoria Flash ROM del BIOS y el contenido de la Shadow RAM después de descompactar el código del BIOS en la RAM.

¿Qué es la Memoria CMOS o CMOS RAM?

La memoria CMOS (Complementary Metal Oxide Semiconductor) es un tipo de circuito de memoria que se caracteriza por su bajo consumo de potencia y relativamente poca capacidad. En el diseño original de los sistemas AT 286, se destinó un circuito de este tipo para almacenar los parámetros de configuración de la PC y se eliminaron los microinterruptores que existían en la XT. En esta memoria se almacenan parámetros tales como el número de unidades, el tipo y tamaño del disco duro, la fecha y la hora del sistema, así como una gran cantidad de otros datos que permiten configurar apropiadamente el sistema y obtener el máximo de sus posibilidades. Aprovechando su bajo consumo de potencia, está alimentada por una batería para mantener la información de la configuración cuando se apaga el sistema.

Algunas consideraciones acerca de la Memoria CMOS

La información que contiene esta memoria se actualiza mediante el programa SETUP del BIOS, el cual se puede activar, normalmente mediante una combinación de teclas (DEL, en los BIOS AMI y AWARD) justo después que el sistema acaba el chequeo de memoria. La información de la configuración del sistema no debe ser

Elementos de Arquitectura y Seguridad Informática

alterada por personal que no esté calificado para ello, porque puede provocar que se afecten las prestaciones de la máquina o que incluso este deje de funcionar completamente.

En algunas Tarjetas Madres la CMOS RAM es alimentada por una Batería de Níquel - Cadmio recargable. Con el tiempo estas baterías suelen sulfatarse y a veces provocan daños irreparables en su sistema. Es recomendable revisar periódicamente el estado de estas baterías y del impreso a su alrededor para poder detectar a tiempo cualquier problema. Este tipo de batería es muy común en los sistemas 386 y 486. En la actualidad los sistemas Pentium vienen con una batería de Litio la cual no presenta esta dificultad.

En algunos BIOS se permite poner palabras claves o contraseñas (Password) que pueden proteger el acceso tanto al sistema como al programa SETUP. En ocasiones, por diferentes motivos, no es posible contar con esta palabra clave y es imposible entrar al sistema o al SETUP. Esto se puede resolver de varias formas:

Revisar el manual de la tarjeta madre, buscando un Jumper que permita deshabilitar el Password. En algunos casos hay que encender la máquina con este Jumper en cierta posición. Es posible que el resto de las opciones del SETUP no se afecten por este procedimiento.

Quitar o desoldar la pila. En este caso es una operación que requiere gran cuidado con el objetivo de no dañar el circuito impreso o la pila. Tiene el inconveniente que se pierde también toda la información que almacenaba el SETUP.

Correr algún programa que corrompe la estructura de la CMOS. Al despertar la computadora, después de ejecutar este programa, detecta que la CMOS no contiene información válida y permite entrar en el SETUP para arreglar este problema. Tiene el inconveniente que se pierde también toda la información que almacenaba el SETUP.

Programa SETUP del BIOS

Una definición técnica de lo que significa el SETUP del BIOS pudiera ser: "Programa, almacenado en la ROM BIOS, que permite cambiar y almacenar los parámetros de la configuración del hardware del sistema en la CMOS RAM".

Pero dicho así, tan "técnicamente", puede ser algo confuso para ciertas personas, que no entienden que cosa es el BIOS, porque es necesario configurar el hardware y mucho menos saben en que consiste dicha configuración.

Expliquémoslo un poco más detalladamente, además del POST y de las rutinas de Entrada/Salida que permiten al Sistema Operativo interactuar directamente con el hardware, en la **ROM BIOS** se almacena un programa especial conocido como **SETUP del BIOS**. Este es el programa que permite cambiar la configuración del hardware, modificando sus parámetros internos de acuerdo a las características y

posibilidades del sistema y almacenarlos posteriormente en la CMOS RAM de su computadora.

Esta configuración es usada por las rutinas del BIOS para manipular los dispositivos del sistema, esto incluye la configuración de la memoria, el Chipset, el CPU, dispositivos de Entrada/Salida, etc. Por esta razón es muy importante que la configuración que se establezca en este programa sea correcta, porque no solamente puede afectar el rendimiento del sistema, sino que puede provocar que este funcione inestablemente o no funcione del todo.

Cuando se introdujo el PC - AT, este incluyó una pila que energizó la memoria CMOS que contiene la información de configuración. La CMOS era originalmente actualizada por un programa sobre el Disco Diagnóstico, sin embargo, posteriormente estas rutinas fueron incorporadas en el BIOS.

Desdichadamente, como los Chipsets controlan a los CPUs modernos, estos han llegado a ser más complejos, la variedad de parámetros especificables en el SETUP ha crecido. Además, ha habido poca estandarización de terminología entre los vendedores de BIOS, los fabricantes de Chipset y un número grande de vendedores de Tarjeta Madre. Las quejas sobre la pobre documentación de la tarjeta madre en cuanto a los parámetros del SETUP, son muy comunes.

Para complicar aún más este problema, algunos parámetros son definidos por los vendedores del BIOS, otros por los diseñadores del chipset, otros por los diseñadores de la tarjeta madre, y otros por diversas combinaciones de los ya mencionados. Los parámetros destinados al uso en el Diseño y el Desarrollo, son mezclados con parámetros destinados para ser ajustados por técnicos - quienes frecuentemente están tan desconcertados por esta materia como todos los demás. Ninguna persona u organización parece comprender todos los parámetros disponibles para cualquier SETUP.

El SETUP se puede ejecutar bajo alguna de las siguientes condiciones:

- El usuario cambia la configuración del sistema producto de incorporar nuevo hardware o para modificar los parámetros ya establecidos.
- El usuario reemplaza la batería de respaldo de la CMOS RAM.
- El sistema detecta un error de configuración y solicita al usuario que ejecute el programa de configuración.

¿Cómo activar el SETUP de su computadora?

Al encender su computadora se efectuará de forma automática un chequeo y conteo de la memoria RAM (se observa este proceso de forma rápida en la pantalla). Apareciendo posteriormente un mensaje que le pedirá presionar una o varias teclas si se desea ejecutar la rutina de configuración SETUP. Estas combinaciones pueden variar según el fabricante del BIOS:

- Tecla DEL para los BIOS AMI y AWARD.

Elementos de Arquitectura y Seguridad Informática

- Ctrl + Alt + Esc para los BIOS ACER.
- F2, ESC, Ctrl + S son otras posibles combinaciones.

Este programa del BIOS deberá ejecutarse inmediatamente después de haber instalado o removido algún periférico en su computadora y se debe presionar esta tecla (o combinaciones de teclas) inmediatamente después del conteo de la memoria, de otra forma se iniciará la carga de S.O, sin haber incluido en la configuración del hardware los cambios efectuados. Siempre que se utiliza el programa SETUP el equipo reiniciará su operación para tomar los nuevos valores que se almacenan en la CMOS RAM.

Teclas de control

La siguiente tabla muestra un resumen de las acciones más frecuentes que pueden realizarse con las teclas de flecha, Esc, PgUp, PgDn y teclas de funciones en el AWARD BIOS SETUP.

Tabla II-2

Flecha Arriba	Moverse a la opción anterior.
Flecha Abajo	Moverse a la próxima opción.
Flecha Izquierda	Móverse a la opción que está a la izquierda.
Flecha Derecha	Moverse a la opción que está a la derecha.
Tecla ESC	Main Menu – Salir y no salvar los cambios en la CMOS. Otras Páginas – Salir de la Página actual y retornar al Menú principal.
Tecla PgUp Tecla +	Incrementa el valor numérico o hace cambios.
Tecla PgDn Tecla -	Decrementa el valor numérico o hace cambios.
Tecla F1	Ayuda general, solo disponible en algunas pantallas y referida fundamentalmente a los valores posibles de las opciones y especifica cual es el implícito para el BIOS y el SETUP.
Tecla (Shift) F2	Permite cambiar la combinación de colores, hasta 16 posibilidades. F2 para cambiarlos en un sentido y Shift + F2 para hacerlo en el sentido contrario.
F3 tecla	Reservado.
F4 tecla	Reservado.

F5 tecla	Restablece el valor anterior de la CMOS.
F6 tecla	Carga los valores implícitos de la CMOS desde la tabla implícita del BIOS.
F7 tecla	Carga los valores implícitos del SETUP.
F8 tecla	Reservado.
F9 tecla	Reservado.
F10 tecla	Salva todos los cambios en la CMOS.

Debido a la gran cantidad de configuraciones y componentes que hay hoy en día, las opciones de ajuste que brinda el BIOS se deben disponer de manera que se adecuen lo máximo posible al conjunto formado por el hardware y el software que constituye el PC. Del ajuste preciso de los parámetros que conforman el Setup del BIOS (ver anexo) depende en buena medida el óptimo funcionamiento del ordenador. Al Setup del BIOS se puede acceder con una determinada configuración de teclas. En la mayoría de los casos se accede apretando la tecla Del durante el POST.

El BIOS reside en memoria ROM y es necesario para el funcionamiento de cualquier PC, esta memoria contiene los programas y los datos que son necesarios para activar y hacer funcionar el ordenador y sus dispositivos periféricos. La ventaja de tener los programas fundamentales del ordenador almacenados en ROM es que están allí implementadas en el interior del ordenador no habiendo necesidad de cargarlas en la memoria desde el disco, de la misma forma en que se carga por ejemplo los Sistemas Operativos. Debido a que están siempre residentes, los programas en ROM son muy a menudo los cimientos sobre los que se construye el resto de los programas. La ROM en un principio (Primeras PC) estaba estructurado en 4 partes de las cuales hoy en día en los sistemas actuales, se prescinden de algunos de ellos, como por ejemplo la ROM-Basic. Solo vamos a hacer mención a las partes antes mencionadas para una mejor comprensión.

Programas de arranque: hacen el trabajo de poner en marcha el ordenador.

ROM – BIOS: es un acrónimo para indicar el sistema de entradas/salidas básico y que está formada por una colección de rutinas en lenguaje de máquina, que proporciona los servicios de soporte para las operaciones del ordenador.

ROM – BASIC: proporciona el núcleo del lenguaje de programación BASIC.

Extensiones ROM: son programas que se añaden a la ROM principal cuando se conectan al ordenador ciertos equipos especiales.

El primer trabajo de los programas en ROM tiene que ser supervisar la puesta en marcha del ordenador. Son varias las tareas realizadas por las rutinas de puesta en marcha. Por ejemplo, ejecutan una comprobación rápida de la fiabilidad del ordenador (y de los programas de la ROM) para estar seguros de que todo está trabajando en orden; inicializan los chips y el equipo estándar conectado al

Elementos de Arquitectura y Seguridad Informática

ordenador; ponen la tabla de los vectores de interrupción; comprueban la existencia de equipo opcional conectado, si está conectado un controlador de disco y se termina cargando el sistema operativo.

El test de fiabilidad, es un primer paso importante que permite estar seguro de que el ordenador se encuentra listo. Todas las rutinas del POST son bastante breves, en tiempo, excepto las que se dedican a realizar los tests de memoria que pudieron ser más largos en dependencia de la cantidad de memoria instalada en el sistema.

Durante la inicialización una rutina pone los valores por defecto de los vectores de interrupción, estos valores por defecto apuntan hacia las rutinas dedicadas al tratamiento de interrupciones, que se encuentran localizadas en el interior de la ROM-BIOS, o apuntan hacia rutinas que no hacen nada, y que los programas suplirán después. Durante esta inicialización se determina que equipo está conectado al ordenador, realizando su inicialización. Esta información es dada al sistema mediante la configuración del setup y almacenada en la CMOS, tal y como explicamos anteriormente.

La parte final del procedimiento de puesta en marcha se denomina cargador boot-strap y es una rutina corta que se emplea para cargar un programa almacenado en medio de almacenamiento.

El cargador boot-strap intenta leer registro de arranque, que está localizado en el disco, si este proceso es satisfactorio pasa el control del ordenador al programa que está incluido en aquel registro. Este programa tiene la tarea de cargar el resto del programa del disco. Normalmente este programa es el SO.

Si el cargador boot-strap no puede leer el registro cargador del disco, (activa en los sistemas antiguos el ROM-Basic), en los nuevos sistemas es emitido el mensaje:

No ROM-Basic, Sistema detenido.

En caso de que alguna de las comprobaciones que efectúa el BIOS al arrancar el ordenador detecte un error, una serie de sonidos son emitidos a través de la bocina, indicando el tipo de fallo que se ha producido.

Estas se pueden resumir de la siguiente manera:

1. beep – DRAM refresh failure (Fallo en el refrescamiento de la DRAM. El circuito de refrescamiento de la memoria ha fallado).
2. beeps – Parity Circuit failure (Fallo de paridad. Se ha detectado un error de paridad en la memoria).
3. beeps – Base 64K RAM failure (Fallo en los 64K de RAM base. Los primeros 64K de la RAM han fallado).
4. beeps – System Timer failure (Fallo en el reloj del sistema. El BIOS ha detectado error en el reloj de la M/B)
5. beeps – Processor failure (Fallo del procesador. La CPU ha dado en error).

6. beeps – Keyboard controller 8042 – Gate A20 Error (Error del controlador 8042 del teclado Gate A20. El BIOS no es capaz de poner a funcionar el CPU en modo protegido).
7. beeps – Virtual Mode Exception Error (Error de excepción en el modo virtual. La CPU ha generado un fallo de interrupción).
8. beeps – Display Memory R/W Test failure (Fallo en el test de escritura y lectura en la memoria de la tarjeta gráfica. Se ha producido un mal funcionamiento en la memoria de la tarjeta gráfica).
9. beeps – ROM – BIOS checksum failure (Fallo de comprobación de la ROM – BIOS. El código de control de la ROM no coincide con el almacenamiento en la BIOS).
10. beeps – CMOS Shutdown Register failure (Fallo en el registro de apagado de la CMOS. El registro de apagado de lectura y escritura de la ROM ha fallado).
11. beeps – Cache Error/External Cache Bad (Error en la memoria cache. La cache externa esta defectuosa).
12. 2 beeps cortos – Post failed (Fallo en el procesador de Post de las test de hardware ha encontrado un error).
13. 1 beep largo y dos cortos – Video failure (Fallo en el adaptador de vídeo. O bien hay un fallo en el ROM de video del BIOS o bien el retraso horizontal del adaptador de video es incorrecto).
14. 1 beep largo y tres cortos – Video failure (Fallo en el adaptador de video. O ha fallado el DAC, o no se ha detectado el monitor o la RAM de video ha dado un error).
15. 1 beep largo – Post Successful (Proceso Post completado con éxito. Todos los tests de hardware han sido completados sin encontrarse error alguno).

Resumiendo: el BIOS proporciona los servicios fundamentales que se necesitan para que se puedan utilizar todas las operaciones del ordenador.

El BIOS controla los dispositivos periféricos del ordenador, todos como la pantalla, el teclado y los controladores de disco, entre otros. De hecho, cuando se utiliza el termino BIOS en su sentido mas riguroso, se hace referencia a los programas encargados de realizar el control de dispositivos.

Estos programas transforman un simple comando tal como por ejemplo: “leer la información de un disco” en todos los pasos necesarios que permita realizar de forma efectiva dicha acción, incluyendo la detección de errores y su conexión. En el sentido mas amplio, el BIOS no solo hace referencia a las rutinas que son necesarias para controlar los dispositivos del PC, sino también hace referencia a las rutinas que contienen información o realizan tareas, que son fundamentales en otros aspectos del funcionamiento del ordenador, como por ejemplo, guardar la hora y el día.

Elementos de Arquitectura y Seguridad Informática

Los programas del BIOS están entre los programas personales y el hardware. En efecto, esto quiere decir que, por un lado, recibe las solicitudes efectuadas por los programas para realizar las secuencias de Entrada/Salida. Estas secuencias se llaman desde los programas mediante combinación de dos números: uno, el de la interrupción (que indica el dispositivo que ha solicitado un servicio) y el otro, el número de servicio (indicando el servicio específico que se debe realizar).

Por otro lado, el BIOS se comunica con los dispositivos (hardware) del ordenador (display, controladores de disco, etc) usando los códigos de control específicos que requiere cada dispositivo. El BIOS también maneja algunas interrupciones de hardware producidas por algún dispositivo. Por ejemplo, siempre que se presiona una tecla, el teclado genera una interrupción que reconoce el BIOS.

Una vez analizado todo lo anterior podemos abarcar el tema de la configuración del setup del BIOS, al cual como dijimos anteriormente se acude mediante combinaciones de teclas durante el POST. A pesar de existir diferentes fabricantes de BIOS, son muy pocas las diferencias entre sus productos.

El Setup se visualiza por parte del usuario para llevar a cabo la configuración del sistema y dentro de él podemos apreciar una serie de menús como por ejemplo:

STANDARD CMOS: SETUP, donde esta la configuración del disco duro, la memoria y el subsistema gráfico.

BIOS FEATURES SETUP: desde aquí se modifican parámetros tan importantes como los caches de primer y segundo nivel, la secuencia de arranque o el "virus warning", opción que debemos desactivar si se va a instalar Win95 o su sistema operativo accede a la interrupción INT 13.

La optimización más importante se encuentra aquí dado la posibilidad de configuración de los caches explicados anteriormente. En este mismo menú se debe verificar si su BIOS no es muy moderna, que Gate A20 option este configurada como Fast y que la video BIOS shadow este habilitada.

CHIPSET FEATURES SETUP: es donde se encuentran la mayoría de las opciones que optimizan sensiblemente el rendimiento de la máquina. Esta opción se conoce también como **ADVANCED CHIPSET SETUP**. Aquí se encuentran todas las opciones que configuran el acceso a memoria.

La mejor recomendación a la hora de cambiar parámetros del BIOS es tener paciencia y conseguir buena cantidad de benchmarks (referencias) para poder medir las prestaciones del sistema. También es bueno aplicar los cambios uno a uno a fin de controlar y acotar tanto la mejora en el rendimiento como las posibles fallas que eventualmente puedan ocurrir, ya que hay opciones que no son compatibles con todas las configuraciones de hardware. Si sigue este método de prueba y error, en el caso que su sistema funcione de manera inestable o no arranque, siempre se puede ir marcha atrás y volver a la situación anterior. En cualquier caso, si no sabe que es

lo que ha cambiado y su sistema no funciona con normalidad, recurra a las opciones:

LOAD BIOS DEFAULTS o **LOAD SETUP DEFAULTS**, para cargar una configuración estable (la del **SETUP** esta ligeramente mas optimizada que la del **BIOS**) que le permitirá arrancar el ordenador y cargar el sistema operativo sin problemas.

También hay micros para configurar la administración de energía o los dispositivos **PCI** y **Plug & Play**, autodetectar los parámetros de los discos duros e introducir y modificar contraseñas que eviten accesos no autorizados tanto al ordenador como a la configuración del **BIOS**.

El **BIOS** actual debe ser un **BIOS** con soporte **Plug & Play (PnP)** y gestion de alimentación para ordenadores con especificaciones **Energy Start (Green)**.

Como aspecto relevante en los **BIOS** actuales se destaca su característica **PnP**. Esto abarca una filosofía de diseño de periféricos como un conjunto de especificaciones de la arquitectura de las **PCs**. El objetivo principal del **PnP** es que se puede montar de forma inteligente los nuevos dispositivos (tarjetas de video, **CDROM**, tarjeta de red, etc) sin requerir la intervención del usuario. Con este sistema, el usuario puede añadir o quitar dispositivos o conectarse y desconectarse de una red o estación sin necesidad de reiniciar el sistema o definir una serie de parámetros. **PnP** detecta automáticamente la existencia de un nuevo dispositivo, determina la configuración optima y permite que las aplicaciones se ajusten a los cambios ocurridos para llevar a cabo todo ello se necesita un hardware con características **PnP**, un periférico **PnP** y un sistema con características también **PnP**.

Los **BIOS** actuales utilizan como soporte una **Flash ROM**. Esta característica permite una actualización del **BIOS** en cuestión. Esta actualización se realiza en el mismo sistema, sin necesidad de extraer dicho **BIOS**.

Por último, si desea que su ordenador arranque mas rápido, ponga como **Boot Sequence** la cadena "C, A", deshabilite el **Boot Up floppy seek** y ponga **Enable** el **Quick Power on Self Test**.

Chipset

El "chipset" es el conjunto (set) de chips que se encargan de controlar determinadas funciones del ordenador, como la forma en que interacciona el microprocesador con la memoria o la caché, o el control de los puertos y slots **ISA**, **PCI**, **AGP**, **USB**...Antiguamente estas funciones eran relativamente sencillas de realizar y el chipset apenas influía en el rendimiento del ordenador, por lo que el chipset era el último elemento al que se concedía importancia a la hora de comprar una placa base, si es que alguien se molestaba siquiera en informarse sobre la naturaleza del mismo.

Chipset: Un juego integrado de chips de [VLSI] que realizan todas las funciones vitales de un sistema de la computadora, incluso las funciones que una vez

Elementos de Arquitectura y Seguridad Informática

requirieron chips separadas. Los tipos de dispositivos reemplazados por el Chipset incluyen:

- Controlador de memoria.
- Controlador de EIDE.
- PCI puente.
- RTC (reloj del real-tiempo).
- Controlador de DMA.
- Controlador de IrDA.
- Controlador del teclado.
- PS/2 controlador del ratón.
- Controlador del Cache secundario.
- Bajo-poder CMOS SRAM.

Todo de información que se guarda en memoria o se envía a cualquier dispositivo de I/O ha atravesado el Chipset en su manera al CPU. Tú puedes pensar en el CPU como un término o nodo, mientras el Chipset es el cubo. El Chipset es todos sobre I/O y [multiplexing] y traslado de los datos. Periféricos necesitan el Chipset para acceder otro Periféricos.

¿Habéis oído hablar tú alguna vez de DMA? ¿Te has preguntado alguna vez cómo las desviaciones de los datos el CPU encendido su manera al dispositivo apropiado? El controlador de DMA dentro del Chipset hace eso. ¿Qué guarda datos que vierte en del disco duro al CPU de chocar con datos de otros dispositivos? Los controladores del bus (memoria, PCI, ISA, EISA) dentro del Chipset haga eso.

El Chipset ejecuta la muestra. Cuando los nuevos Chipsets surgen, los fabricantes del motherboard rediseñan sus tablas para acomodarlos. Presentemente, más Chipsets están teniendo funcionalidad mayor, así como los costes están quedándose relativamente constante.

El CPU puede cambiarse. La memoria puede actualizarse. El disco duro puede cambalachearse. Pero el motherboard se ha diseñado alrededor de las capacidades del Chipset, y hasta que tú cambie el motherboard, su PC funcionará grandemente el mismo.

Aquí están algunos ejemplos de qué propiedades los dictados del Chipset:

- Tipo de memoria: FPM, EDO, BEDO, SDRAM, paridad - verificando, ECC,
- Cache secundario: el Ráfaga (Bursts), la tubería estalló, síncrono, asíncrono
- CPU teclean: 486, P-24T, P5, P54C/P55C, Pentium En pro de, Pentium II

- Máximo memoria bus velocidad: 33, 40, 50, 60, 66, 75, 83, 100 MHz,
- PCI bus [synch]: síncrono o asíncrono a velocidad de bus de memoria
- PCI bus tipo: 32-bit o 64-bit
- Capacidad de SMP: solo, dual, trío.
- Apoye para los rasgos gusta: AGP, IrDA, USB, PS/2 ratón,
- Apoyo para construir-en PCI controlador de EIDE y cada posibles EIDE ofrecen tú podéis imaginar: el modo de DMA, modo de PIO, ATA/33, etc.,
- Construir en PS/2 ratón, controlador del teclado y BIOS, y circuitería de reloj de real-tiempo.

Como se puede observar, mucho de lo que hace un buen Chipset es que, puede reemplazar las docenas de chips que marcaban una motherboard y requerían compatibilidad detallada, qué prueba para los diseñadores del motherboard. Con un solo chip o con dos chips , muchos Chipsets pueden reemplazar casi todos los chips que anteriormente se usaban, controlando la motherboard.

Pero los nuevos y muy complejos micros, junto con un muy amplio abanico de tecnologías en materia de memorias, caché y periféricos que aparecen y desaparecen casi de mes en mes, han hecho que la importancia del chipset crezca enormemente. De la calidad y características del chipset dependerán:

- Obtener o no el máximo rendimiento del microprocesador.
- Las posibilidades de actualización del ordenador.
- El uso de ciertas tecnologías más avanzadas de memorias y periféricos.

Es el responsable de la comunicación entre los componentes de la placa base, los componentes que se conectan a ella (memoria, tarjeta gráfica, tarjetas SCSI, etc.) y con los periféricos (disco duro, disketera, puertos serie, paralelo, USB e infrarrojos). Las transacciones entre el procesador y la memoria y el resto de los componentes internos o externos pasa por el CHIPSET, e integra las siguientes funciones:

- Controladora de memoria.
- Controladora IDE.
- Puente PCI.
- Reloj en tiempo real (RTC).
- Controladora de acceso directo a memoria (DMA).
- Controladora de puerto de infrarrojos (IrDA).
- Controladora de teclado.
- Controladora de ratón PS/2.
- Controladora de caché de segundo nivel.

Elementos de Arquitectura y Seguridad Informática

Es obvio que de su elección depende en gran parte el rendimiento del equipo, pero el diseño de la propia placa base (que varía de un fabricante a otro, de modelo a modelo e incluso dentro de las distintas versiones de cada modelo) es el que puede sacar o no el máximo provecho al chipset utilizado.

Trataremos sólo los chipsets para Pentium y superior, ya que el chipset de un 486 o inferior no es de mayor importancia (dentro de un límite razonable) por estar en general todos en un nivel similar de prestaciones y rendimiento, además de totalmente descatalogados. Tampoco trataremos todas las marcas, sino sólo las más conocidas o de más interés; de cualquier forma, muchas veces se encuentran chipsets aparentemente desconocidos que no son sino chipsets VIA, ALI o SIS bajo otra marca.

Chipsets para Pentium y Pentium MMX

De Intel (Tritones)

Fue la primera (y muy exitosa) incursión de Intel en el mundo de los chipsets. Esto no resulta extraño, ya que nadie mejor que Intel conoce cómo sacar partido a sus microprocesadores; además, el resto de fabricantes dependen de la información técnica que les suministra Intel.

430 FX: el Tritón clásico, de apabullante éxito. Un chipset bastante apropiado para los Pentium "normales" (no MMX) con memorias tipo EDO. Hoy en día desfasado y descatalogado.

430 HX: el Tritón II, la opción profesional del anterior. Mucho más rápido y con soporte para placas duales (con 2 micros). Algo anticuado pero muy bueno.

430 VX: ¿el Tritón III? Más bien el 2.5; algo más lento que el HX, pero con soporte para memoria SDRAM. Se puede decir que es la revisión del FX, o bien que se sacó para que la gente no se asustara del precio del HX...

430 TX: el último chipset de Intel para placas Pentium (placas socket 7). Si queremos usar micros Intel y aplicaciones que se contenten con placas con 1 Pentium, la opción a elegir. Soporte MMX, SDRAM, UltraDMA... Un problema: si se le pone más de 64 MB de RAM, la caché deja de actuar; aunque más de 64 MB es mucha RAM.

Tabla II-3

Chipsets de Intel para Pentium y Pentium MMX				
Concepto	430 FX	430 HX	430 VX	430 TX
Número CPUs máx.	1	2	1	1
RAM máxima	128 MB	512 MB	128 MB	256 MB

Tipos de RAM	FPM, EDO		FPM, EDO, SDRAM
RAM cacheable máxima	64 MB	512 MB (según placa, no todas)	64 MB
Caché L2 máxima	512 KB		
Velocidad bus máx.	66 MHz		
Puertos adicionales		USB	UltraDMA y USB
Comentarios	Desfasado	No adecuados para micros no Intel de nueva generación (no soportan AGP ni bus 100 MHz)	

Lo más destacable de estos chipsets, su buen rendimiento, especialmente con micros Intel. Lo peor, su escaso soporte para micros no Intel, que en el campo socket 7 tienen desarrollos superiores a los de Intel, como los AMD K6 (normal y K6-2) o los Cyrix-IBM 6x86MX (M2), en general más avanzados que los Pentium y Pentium MMX.

De VIA (Apollos)



Unos chipsets bastante buenos, se caracterizan por tener soporte para casi todo lo imaginable (memorias SDRAM o BEDO, UltraDMA, USB...); su pelea está en la gama del HX o TX, aunque suelen ser algo más lentos que éstos al equiparlos con micros Intel, no así con micros de AMD o Cyrix-IBM (Figura II.5).

Figura II.5. Chipset de Via.

Tabla II-4

Chipsets de VIA para Pentium y Pentium MMX				
Concepto	VP2	VPX	VP3	MVP3
Número CPUs máx.	1			
RAM máxima	512 MB		1 GB	
Tipos de RAM	FPM, EDO, BEDO, SDRAM		FPM, EDO, SDRAM	

Elementos de Arquitectura y Seguridad Informática

RAM cacheable máxima	512 MB (según placa, no todas)		512 MB ó 1 GB (según placa, no todas)	
Caché máxima L2	2048 KB			
Velocidad bus máx.	66 MHz	75 MHz	66 MHz	100 MHz
Puertos adicionales	UltraDMA y USB		UltraDMA, USB y AGP	
Comentarios	No adecuados para micros no Intel de nueva generación (no soportan AGP ni bus 100 MHz)		Sin bus a 100 MHz	Muy moderno, con todos los avances

Lo bueno de las placas con chipsets VIA es que siguen en el mercado socket 7, por lo que tienen soporte para todas las nuevas tecnologías como el AGP o los buses a 100 MHz, además de que su calidad suele ser intermedia-alta. En las placas con chipsets Intel hay un abanico muy amplio entre placas muy buenas y otras francamente malas, además de estar ya desfasadas (ningún chipset Intel para socket 7 soporta AGP, por ejemplo).

El último chipset de VIA para socket 7, el MPV3, ofrece todas las prestaciones del BX de Intel (excepto soporte para placas duales), configurando lo que se denomina una placa Super 7 (con AGP y bus a 100 MHz), que con un micro como el nuevo AMD K6-2 no tiene nada que envidiar a un equipo con Pentium II.

De ALI

Muy buenos chipsets, tienen soluciones tan avanzadas como el chipset para placas Super 7 "Aladdin V", que como el MPV3 de VIA resulta equiparable a todos los efectos al BX de Intel para placas Pentium II (bus a 100 MHz, AGP...); una fantástica elección para micros como el AMD K6-2. (Ver tabla para Chipset de Ali)

De SiS

Como los anteriores, sus capacidades son avanzadas, aunque su velocidad sea a veces algo más reducida que en los de Intel. Resultan recomendables para su uso junto a chips compatibles Intel como el K6 de AMD o el 6x86MX (M2) de Cyrix-IBM, aunque desgraciadamente no soportan por ahora el bus a 100 MHz del nuevo K6-2. (Ver tabla para de Chipset de SiS.)

Tabla II-5

Chipsets de ALI para Pentium y Pentium MMX			
Concepto	M1521/M1523 (Aladdin III)	M1531/M15X3 (Aladdin IV-IV+)	M1541/M1543 (Aladdin V)
Número CPUs máx.	1		
RAM máxima	1 GB		
Tipos de RAM	FPM, EDO, SDRAM		FPM, EDO, SDRAM, PC100
RAM cacheable máxima	512 MB (según placa, no todas)		
Caché L2 máxima	1 MB		
Velocidad bus máx.	75 MHz	83,3 MHz	100 MHz
Puertos adicionales	USB	UltraDMA y USB	UltraDMA, USB y AGP
Comentarios	Apropiados para micros no Intel pero no de última generación (AMD K6-2) por carecer de bus a 100 MHz		Muy moderna, con todos los avances

Tabla II-6

Chipsets de SIS para Pentium y Pentium MMX			
Concepto	5597/5598	5581/5582	5591/5592
Número CPUs máx.	1		
RAM máxima	384 MB		768 MB
Tipos de RAM	FPM, EDO, SDRAM		
RAM cacheable máxima	128 MB		256 MB
Caché L2 máxima	512 KB		1 MB
Velocidad bus máx.	75 MHz		83 MHz
Puertos adicionales	UltraDMA, USB y SVGA integrada	UltraDMA y USB	UltraDMA, USB y AGP
Comentarios	Apropiados para micros no Intel (especialmente Cyrix) pero no los de última generación (AMD K6-2) por carecer de bus a 100 MHz		

Chipsets para Pentium II y Celeron

De Intel

Son bastante avanzados, excepto el anticuado 440 FX (que no es propiamente un chipset para Pentium II, sino más bien para el extinto Pentium Pro) y el barato EX, basado en el LX pero con casi todas las capacidades reducidas (Figura II.6).

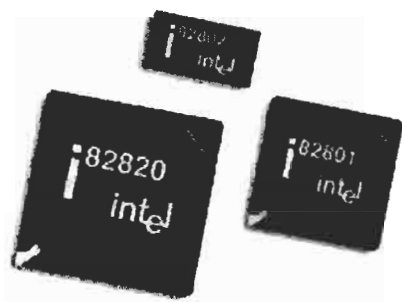


Figura II.6. Vista de Chipset de Intel.

Tabla II-7

Chipsets de Intel para Pentium II y Celeron				
Concepto	440 FX	440 LX	440 BX	440 EX
Número CPUs máx.	2			1
RAM máxima	512 MB	1 GB EDO ó 512 MB SDRAM	1 GB	256 MB
Tipos de RAM	FPM, EDO	FPM, EDO, SDRAM	SDRAM y PC100 SDRAM	FPM, EDO, SDRAM
RAM cacheable máxima	No aplicable (dentro del microprocesador, tamaño fijo)			
Caché L2 máxima				
Velocidad bus máx.	66 MHz		100 MHz	66 MHz
Puertos adicionales	UltraDMA y USB	UltraDMA, USB y AGP		

Comentarios	Desfasado			Apropiado sólo para Celeron
-------------	-----------	--	--	-----------------------------

Tipos de buses

¿Qué es un Bus? - Es un standard de comunicación, un acuerdo acerca de cómo construir tarjetas que puedan trabajar en una PC standard. Sin embargo, por diversas razones no solo existe un standard sino cuatro diferentes en el mundo de las PC además de algunos fuera de lo común.

En el bus se encuentran dos pistas separadas, el bus de datos y el bus de direcciones. La CPU escribe la dirección de la posición deseada de la memoria en el bus de direcciones accediendo a la memoria, teniendo cada una de las líneas carácter binario. Es decir solo pueden representar 0 o 1 y de esta manera forman conjuntamente el numero de la posición dentro de la memoria (es decir: la dirección). Cuanto más líneas haya disponibles, mayor es la dirección máxima y mayor es la memoria a la cual puede dirigirse de esta forma. En el bus de direcciones original habían ya 20 direcciones, ya que con 20 bits se puede dirigir a una memoria de 1 MB y esto era exactamente lo que correspondía a la CPU. Esto que en la teoría parece tan fácil es bastante más complicado en la práctica, ya que aparte de los bus de datos y de direcciones existen también casi dos docenas más de líneas de señal en la comunicación entre la CPU y la memoria, a las cuales también se acude. Todas las tarjetas del bus escuchan, y se tendrá que encontrar en primer lugar una tarjeta que mediante el envío de una señal adecuada indique a la CPU que es responsable de la dirección que se ha introducido. Las demás tarjetas se desprecupan del resto de la comunicación y quedan a la espera del próximo ciclo de transporte de datos que quizás les incumba a ellas. (Ver tabla acerca de los microprocesadores y los buses)

Este mismo concepto es también la razón por la cual al utilizar tarjetas de ampliación en una PC surgen problemas una y otra vez, si hay dos tarjetas que reclaman para ellas el mismo campo de dirección o campos de dirección que se solapan entre ellos.

Los datos en si no se mandan al bus de direcciones sino al bus de datos. El bus XT tenía solo 8 bits con lo cual sólo podía transportar 1 byte a la vez. Si la CPU quería depositar el contenido de un registro de 16 bits o por valor de 16 bits, tenía que desdobarlos en dos bytes y efectuar la transferencia de datos uno detrás de otro.

De todas maneras para los fabricantes de tarjetas de ampliación, cuyos productos deben atenderse a este protocolo, es de una importancia básica la regulación del tiempo de las señales del bus, para poder trabajar de forma inmejorable con la PC. Pero precisamente este protocolo no ha sido nunca publicado por IBM con lo que se obliga a los fabricantes a medir las señales con la ayuda de tarjetas ya existentes e imitarlas. Por lo tanto no es de extrañar que se pusieran en juego tolerancias que dejaron algunas tarjetas totalmente eliminadas.

Elementos de Arquitectura y Seguridad Informática

Buses establecidos: Cuatro tipos de buses han sido históricamente preestablecidos en las microcomputadoras de manera clásica: el ISA de 8 bits, el ISA de 16 bits, el MCA desarrollado por IBM y el bus EISA.

Tabla II-8

PROCESADOR	Bus de direcciones	Bus de datos
8086	20	16
8088	20	8
80186	20	16
80188	20	8
80286	24	16
80386 SX	32	16
80386 DX	32	32
80486 DX	32	32
80486 SX	32	32
PENTIUM	32	64
PENTIUM PRO	32	64

Bus ISA/AT (Industrial Estándar Architecture)

El bus ISA fue el del primer surgimiento en una temprana versión de 8 bits de datos y 20 para llevar a cabo el direccionamiento (en sus dos formas: dirección de memoria y dirección de puerto de E/S)

Con la introducción de los modelos AT por IBM el bus fue adaptado a las nuevas capacidades de los microprocesadores. A las 8 líneas ya presentes en el bus de la computadora se le adicionaron otros 8 adicionales, resultando un ancho de datos de 16 bits. Las líneas de dirección se ampliaron de 20 a 24, haciendo posible acceder hasta 16 MB. También se adicionaron líneas de control que indican al MPU si los próximos datos se transferirán en un formato de 8 o 16 bits, si antes de iniciar la transmisión la tarjeta ha indicado que es de 16 bits. Aunque la compatibilidad del bus ISA/AT es práctica en teoría, tiene la desventaja de que la tarjeta de expansión de 16 bits debe dar la señal necesaria antes de iniciar la transferencia.

Para una respuesta rápida de la tarjeta ante una solicitud se adiciona un intercambio especial. Cuatro líneas de dirección son duplicadas, pero con una instantánea descodificación que permite reconocer a la tarjeta que esta en uso. Líneas adicionales para las interrupciones y el control del acceso directo a memoria (DMA) fueron establecidas. También se adiciono una línea de master sobre el bus que permite que la tarjeta de expansión tome el control de toda la computadora, acción sin embargo algo lenta en su establecimiento; por lo que solo es recomendable para que tome el control otro MPU.

A pesar de su atadura a 8 MHz, su poca flexibilidad para multiprocesamiento, su baja razón de transferencia (6,5 Mb/s) supo sobrevivir a sus competidores en parte debido al gran volumen de soporte con que contó y su alta estandarización y en

parte por el alto costo frente al relativo bajo nivel de prestaciones de sus competidores. Los sistemas 80386 y 80486 requerían cambios drásticos en la arquitectura del bus. El bus de datos de 16 bits y el direccionamiento de 24 bits del bus AT no satisface las bondades de los nuevos procesadores, los cuales prefieren un bus de datos y direcciones de 32 bits.

Bus MCA

El bus Micro Channel (MCA) fue introducido por IBM en 1987, conjuntamente con los módulos PS/2. Este bus es completamente incompatible con el ISA en cualquier variante, lo que representa que desafortunadamente ninguna tarjeta ISA puede usarse en una computadora con bus MCA, pero ha permitido ir a un rediseño total del bus haciéndolo más rápido y sencillo.

El bus MCA es implementado para 16 bits en microcomputadoras 286 y 386SX y en 32 bits para modelos 386DX y 486. Existen por tanto tarjetas de expansión de 16 y 32 bits. Este bus es asíncronico en su funcionamiento.

Un bus asíncronico toma la frecuencia de reloj a partir de las unidades que participan en la transferencia, pues la unidad receptora reporta la captura del dato a la unidad transmisora y solicita el envío de nuevos datos desde allí. Esto tiende a complicar la estructura del bus pero incrementa su potencialidad. El bus fue diseñado para soportar una razón de transferencia de hasta 20 Mb/s, pero recientes implementaciones alcanzan valores en teoría de hasta 160 Mb/s. El esquema de interrupciones de un bus MCA es superior al del ISA, pues aunque las interrupciones son controladas por el flanco, son marcadas, lo cual redundante en una efectividad que incrementa las posibilidades de sistemas con numerosas interrupciones.

El MCA representa una mejora importante sobre el bus AT y aunque las diferencias son eminentemente técnicas podemos enumerar algunas diferencias importantes:

El MCA ofrece configuración automática al insertar alguna tarjeta en la computadora y correr un programa que involucre el uso de esta tarjeta, no es necesaria ninguna configuración especial. En el bus AT, muchas tarjetas requerían la asistencia técnica de un manual y la configuración por medio de switches o jumpers en la tarjeta en sí. Las tarjetas y los sistemas MCA no necesitan ser configurados con jumpers e interruptores DIP, pues poseen un número de identificación incambiable llamado POS (Programmable Option Select); el cual hace la identificación más fácil al usarse un archivo llamado ADS en el cual todas las configuraciones de tarjetas son almacenadas. El MCA utiliza adaptadores que generan menor interferencia eléctrica que los viejos adaptadores, lo que suministra mayor integridad de datos. El MCA responde mejor a solicitudes de interrupciones. El MCA suministra adaptadores especiales llamados bus masters, que contienen sus propios procesadores y pueden efectuar su trabajo en forma independiente al microprocesador principal.

Por ejemplo, una red puede tener un bus master de fax en su computadora principal (server) de modo que los fax recibido puedan ser impresos en la impresora

Elementos de Arquitectura y Seguridad Informática

de la red, sin distraer la atención del microprocesador principal, lo que provocaría el alentamiento de la red. Dentro de una red, el MCA permite identificar cada adaptador en cada computadora sin necesidad de abrir la cubierta. El MCA tiene la facilidad de apagar un adaptador que este funcionando mal desde un punto remoto.

Aunque MCA fue introducido por IBM en las computadoras PS/2, la estrategia de IBM fue incluir el MCA en otras computadoras tales como estaciones científicas y Main Frames. Aunque la tecnología MCA puede ser técnicamente avanzada, tiene varias desventajas. Es incompatible con las tarjetas de expansión PC AT. Además siendo tecnología propietaria de IBM, su precio es elevado por los regalías que los fabricantes deben pagar.

Características físicas

El bus permite algunas variaciones: implementación de 16-bit, implementación de 32-bit; extensión opcional que permite incrementar la velocidad del bus.

Se reduce las dimensiones de las tarjetas de expansión en comparación con las AT (4.75x13.5 de AT por 3.5x11.5 pulgadas). Esto es posible porque se usan componentes y conectores más pequeños. Estos componentes requieren de menos energía, liberan menos calor y se logra una mayor minituarización.

En este bus existe una redistribución completa de las señales. Cada cuatro pines hay una tierra. La existencia de varias señales de tierra y su proximidad a señales digitales de alta frecuencia reducen más la interferencia en comparación con las PC o AT. Este mejor arreglo de las señales permite también el incremento de la máxima velocidad con las cuales las tarjetas de expansión pueden trabajar, porque se incrementa además el ancho de datos del bus. De hecho, después de una revisión de este bus realizado en 1990, algunos test muestran que este bus puede operar hasta velocidades de 80Mhz.

Descripción de las señales del bus

El MCA usa señales especiales para identificar el ancho de cada tarjeta de expansión que se inserta en el conector (Card Data Size 16 y Card Data Size 32).

Se usan señales Byte Enable Bits 0 al 3 para identificar el tipo de dato que es transferido a través del bus. Así, se puede mover información de 8, 16, 24, 32 bits de una sola vez sin ambigüedades.

La señal Memory Address Enable 24 se usa para indicar si estamos usando el rango de 24 bit del 80286 o el rango de direccionamiento de 32 bit del 80386 y superiores.

En vez de usar líneas separadas para operaciones de memoria y de I/O como hace el bus de PC, el MCA usa una combinación de tres señales Memory/Input-Output, Status Bit One y Status Bit Two para definir el tipo de ciclo de bus a realizar.

Otras extensiones permiten integrar un canal simple de señal analoga de audio de fidelidad media ej: voz sintetizada, música con la estructura del bus IBM.

La extensión de video del MCA permite a las tarjetas de expansión acceder al circuito de video gráfico (VGA) construido dentro de algunas tarjetas madres.

La extensión de video de MCA habilita la conexión del coprocesador de video de su tarjeta en su sistema y permite tener conectado su monitor a su coprocesador de video sin necesidad de un cable adicional. Esto no ocurre con las máquinas no MCA.

La extensión de video tiene otras importantes señales. Están presentes las señales de sincronismo horizontal y vertical , una señal especial de control de línea llamada ESYNC o Enable Sync. Esta línea determina si la señal de sincronismo usada en el video es originada en la tarjeta madre o en otro adaptador conectado en el MCA.

El dato de video que es transferido a través de la extensión de video se realiza en forma digital usando ocho líneas de datos de video. El dato aquí, se suele llevar de VGA digital a analoga en el sistema de tarjeta.

Se tiene dos señales de reloj y una señal especial de blanking.

Para lograr una mayor efectividad en el manejo del sistema se agregan nuevas líneas ej: Card Select Feedback, Channel Ready Line, Channel Ready Return, etc.

Card Select Feedback: es una señal proveniente de la tarjeta de expansión donde indica que dicha tarjeta está en la dirección que se suponía que esté.

Channel Ready Line: es usada por los dispositivos conectados al bus para solicitar más tiempo (no mayor de 3.5 microseg) para completar una operación.

Channel Ready Return: es usada para monitorear la señal anterior cuando todas ellas indican que no necesitan tiempo adicional.

El MCA permite un nuevo modo de transferencia de datos llamado Matched Memory. Cuando la memoria y los periféricos internos de 16 o 32 bit pueden trabajar a velocidades superiores se introducen pulsos adicionales acelerados para la transferencia de datos permitiendo una mejora en el rendimiento de un 25%.

Arbitraje del bus

Este ha sido el aspecto de mayor salto en comparación con el diseño de la tradicional PC. Este arbitraje permite no solo la multitarea, sino también el procesamiento paralelo.

La AT permite compartir el bus, pero requiere de un software especial para controlar el sistema. A través de la programación se realiza la prioridad y al programador se le da cierta responsabilidad. Con el MCA todo el trabajo de arbitraje es realizado por el hardware con un mínimo de soporte de software. Solo se requieren algunos ciclos de bus, sin embargo en un esquema por software se requiere de un número de instrucciones de programa y por ende de más ciclos de reloj.

Elementos de Arquitectura y Seguridad Informática

El MCA toma el control del bus del sistema del microprocesador y se lo da a un circuito llamado por IBM Punto de Arbitraje Central (PAC). Las transferencias a través del bus son manejadas por dispositivos llamados bus masters. Se permiten múltiples bus masters y el bus provee de un método jerárquico y dinámico para las prioridades y acceder a cada master. Para la implementación de esta estrategia de arbitraje el MCA usa varias líneas. Cuatro de ellas Arbitration Bus Priority Levels 0 a 3 llevan el código del nivel de prioridad asignada a cada dispositivo permitiendo 16 niveles de prioridad.

Dos niveles de prioridad son usados por los dispositivos en la tarjeta madre y no aparecen en el MCA. Son niveles especiales usados para darle máxima prioridad al refrescamiento de memoria y a las interrupciones no enmascarables.

Otras tres señales son usadas en el arbitraje del bus:

Pre-empt es usada en el arbitraje para indicar que requiere acceso de MCA.

Arbitrate/Grant es enviado por el PAC para empezar el acceso al bus.

La señal Burst permite a los dispositivos micro canal retener el control para la transferencia múltiple de bloques de datos hasta el final sin recurrir al arbitraje.

Modos secuenciales de transferencia.

Debido a que muchas aplicaciones requieren a menudo realizar transferencias de largas cadenas secuenciales de datos, el MCA implementó el burst mode. Este modo permite a un dispositivo mantener el control del bus sin renegociación por un tiempo no mayor de 12 miliseg. Aún en este Burst mode todas las transferencias de microcanal requieren de dos ciclos de reloj -uno para el direccionamiento, otro para transferir el dato. Para hacer más competitivo este bus con el EISA IBM adicionó un protocolo de transferencias de datos más rápido, que superaba al burst mode llamado streaming data mode.

Interrupciones

En el MCA se realiza el cambio de activación por flanco por el de activación por nivel de las interrupciones. Esto simplifica el diseño del circuito lógico de compartición de las interrupciones en las tarjetas de expansión. Además, esto reduce la sensibilidad del controlador de interrupciones al ruido y a los cambios transitorios y permite la mezcla de equipamiento compartido y no compartido en un mismo nivel de interrupción.

En el MCA, las interrupciones están dedicadas a los mismos objetivos como en el ISA.

Bus EISA (Extended Industry Estándar Architecture)

Muy pocos fabricantes dieron la mano a IBM y en lugar de ello, su respuesta fue la unión de 9 fabricantes (AST, COMPAQ, EPSON, HP, NEC, OLIVETTI, TANDY, WYSE y ZENITH) para la creación de una alternativa para MCA. Esta alternativa fue llamada EISA. Primeramente EISA es compatible con ISA al estar basado en este, soportando tarjetas desarrolladas para este.

El bus EISA posee una estructura de dos niveles, que en su primera etapa es idéntica al bus ISA y en su nivel inferior contiene las conexiones propias del EISA, a las cuales tendrán acceso por su diseño físico las tarjetas como EISA. Al mantener la compatibilidad con el bus ISA, se mantuvo la misma frecuencia de reloj de 8 MHz para los 32 bits de datos y 32 bits de direcciones que soporta el bus. Con este bus es posible lograr transferir hasta 33 Mb/s, si alcanza direccionar hasta 4 Gbytes y hasta 15 dispositivos pueden alcanzar la condición de amos del bus. Otro aspecto novedoso del bus EISA es que las líneas de interrupción pueden ser usadas en común porque no están controladas por el flanco sino por marcado, tal como ocurre en el bus MCA. Las posibilidades de control total (master) sobre el bus son ampliadas con este bus. Ahora el dispositivo master del bus puede tomar rápidamente el control de este y transferir datos entre las unidades aun cuando sean de diferente ancho en su bus de datos.

Cada tarjeta EISA posee un código fijo que es asignado por la asociación EISA y que es leído por el microprocesador para determinar donde la tarjeta se encuentra y simplifica la configuración de la electrónica y la programación. Al desarrollar el circuito 82350 y su familia, INTEL creó el primer conjunto de elementos desarrollados acorde a las especificaciones EISA. El 82357 ISP (Integrated System Peripheral) maneja las funciones del DMA del sistema de forma similar al bus ISA, refrescando además las direcciones de memoria cuando el bus está disponible y soportando el múltiple control del bus, utilizando algoritmos para el reparto de los derechos de control sobre el bus. Posee canales de DMA de 32 bits, cinco contadores de 16 bits para la frecuencia del reloj y ocho canales controladores de canales de interrupción.

El controlador del bus 82385 es el director del bus EISA que permite manejar amos y esclavos en anchos de 8, 16 y 32 bits, regulando las conexiones entre el CPU principal y el bus, y resolviendo cualquier incompatibilidad de datos. Aunque este circuito no es imprescindible su ventaja está en combinar los varios modos de trabajo de este protocolo, asegurando un búfereado efectivo de todos los datos.

El 82355 llamado BMIC o Bus Master Interface Circuit está integrado en una tarjeta de expansión y permite la utilización de las mejores posibilidades del bus EISA al asumir el control de este y garantizar su operación asincrónica, siendo su trabajo tan complejo como el del microprocesador central.

El "Bus Mastering" aprovecha al máximo la especificación EISA para tarjetas externas. Estas tarjetas dedicadas a video o controladores de driver facilitan el trabajo del CPU liberándolos de otras tareas. Actualmente, se continúan los trabajos

Elementos de Arquitectura y Seguridad Informática

en la mejora de la especificación, prediciéndose que al final, se alcanzará en los sistemas EISA la alta velocidad de 66 MB/s contra el límite actual de 33 MB/s.

El bus EISA se justifica para redes con altas razones de transferencia, controladores de disco duro con alto volumen de datos y cache de discos y tarjetas gráficas con muy altas resoluciones.

Características físicas

Las tarjetas de expansión EISA tienen similares medidas y forma que las tarjetas AT(13.4 pulgadas de largo y 4.5 pulgadas de alto).

Las tarjetas EISA se ajustan mejor que las AT.

Adiciona 90 nuevas conexiones (55 nuevas señales) sin incremento de las medidas del conector y aceptando tanto las tarjetas EISA como las AT.

En el nuevo conector los contactos para las funciones mejoradas están construidas dentro del segundo, a un nivel inferior.

Las tarjetas EISA (aunque entren en un conector AT) no deben conectarse a los no EISA conectores porque se enviarán señales hacia circuitos equivocados que podrían dañarlos.

Señales del bus

EISA adicionó 16 nuevas líneas de datos y 8 nuevas líneas de direcciones que permitieron alcanzar los 32-bit de datos y los 32 bit de direcciones(para un alcance de 4Gbytes). Las señales Enable(BE0 aBE4) se utilizan para indicar los bytes de la doble palabra en el bus que son significativos. EISA permite un alcance del DMA a todos los 4GB de direccionamiento de memoria (esto no lo permite el MCA). Para indicar el ancho de datos que soportan los dispositivos, estos envían las señales EX32(acceso de 32 bit de datos) o EX16(transferencia de 16 bit de datos), y en ausencia de ambas el sistema asume que el dispositivo solo puede manejar 8 bit de datos.

Modos de transferencia avanzados

Otras mejoras de EISA requieren de nuevas señales. Estas incluyen a aquellas que dan soporte al burst mode de transferencia de datos(MBURST y SLBURTS), nuevas señales de atiempamiento para ayudar en el manejo de transferencias de datos rápidos (START y CMD) e incluso señales para reducir la velocidad del bus introduciendo estados de espera (EXRDY). Con EISA, todas las señales en el clásico bus retienen sus viejas definiciones y funciones.

La velocidad del bus es un submúltiplo de la frecuencia del reloj del sistema porque EISA es nominalmente un bus sincrónico, él opera unido con el microprocesador

Elementos de Arquitectura y Seguridad Informática

EISA tiene establecidas reglas mucho más pragmáticas y determinísticas para la prioridad.

El control se alterna a través de tres clases: refrescamiento de memoria, transferencia de DMA, y la combinación del microprocesador y el bus master. En cada ciclo de control, cada elemento recibe el control en turno. En cada ciclo de arbitraje, el sistema selecciona uno de la columna A, refrescamiento de memoria; uno de la columna B, DMA; y uno de la columna C, el bus master/ microprocesador. El refrescamiento de memoria tiene asignada la mayor prioridad en el sistema EISA. Cada ciclo de arbitraje incluye refrescar la memoria. Las transferencias de DMA siguen en el orden de prioridad. El microprocesador tiene el siguiente nivel de prioridad.

En la realización del arbitraje intervienen señales como:

Memory Request (MREQ_x, donde x es el número del slot) y se utiliza por la tarjeta del bus master para solicitar acceso al bus. Memory Acknowledge (MAK_x): A través de esta señal el ISP informa al bus máster que puede tomar el control del bus. El estándar EISA también permite la forma de bus máster usada en el bus AT. Estas tarjetas usan las señales de DMA para controlar el bus. DRQ: se solicita el bus. DAR: se le da el permiso para usar el bus.

Interrupciones

El sistema EISA permite que las viejas tarjetas usen las interrupciones por flanco que ellos prefieran, una tarjeta por interrupción. Las nuevas tarjetas EISA pueden compartir otras interrupciones programadas usando la activación por nivel. EISA soporta solo compartir las interrupciones para tarjetas EISA. Las tarjetas AT existentes no pueden compartir interrupciones con otras o con tarjeta EISA.

Bus Local:

Existen 2 estándar de bus local que actualmente compite por su interés. Uno es el VESA o VL-BUS (Video Electronics Estándar Association), el otro PCI (Peripheral Component Interconnect), en este caso una tecnología de INTEL. Ambos logran un ancho de banda entrada/salida mucho mayor para sus periféricos. Tanto uno como el otro logran esto aumentando la velocidad del bus y rompiendo la barrera de los 8 MHz de reloj y los 16 bits de datos originaría de la época de los IBM AT.

Además ambas especificaciones soportan, de una forma o de otra un amplio espectro de prestaciones avanzadas como lo son compartir interrupciones, arbitraje de bus, transferencias en bloques, etc.

Bus Local: Es aquel que está conectado directamente al procesador de su tarjeta madre. La tarjetas que se conectan en los slots de la PC trabajan como si estuvieran

conectadas a este procesador, usando su mismo ancho de banda y velocidad de operación.

VESA o VL- Bus

En 1992 la Video Electronics Standards Association desarrolló un nuevo diseño unificado de BUS local, conocido como VESA o VL-BUS, una tecnología de 32 bits, pero que también puede manejar 16 bits. Las especificaciones VESA están destinadas a una gama amplia de periféricos que requieran altas razones de transferencias como discos duros de alta capacidad, controladores de red y claro, tarjetas de video. Por supuesto, la especificación incluye una detallada descripción de cada señal del BUS lo que hizo posible la aparición inmediata de una gran cantidad de tarjetas que cumplieran dicha normativa.

El BUS VESA es un diseño hecho para complementar más que para sustituir a los diseños actuales. Posee una única línea de interrupciones (IRQ 9), que es usada para engancharse a los otros Buses (ISA, EISA o MCA según el caso) y de esa forma poder utilizar todos sus recursos: interrupciones, controles de DMA, etc. Si el BUS al que está vinculado el VESA soporta interrupciones por flanco en vez de por nivel, entonces también puede utilizar este tipo de interrupciones. Es por ello que VESA se ve más ligado a una "extensión" de los Buses actuales que a un BUS independiente.

Desde el punto de vista de sus señales el VL-BUS virtualmente duplica todo el conjunto de líneas que necesita el procesador 486, a excepción de algunas pocas para buscar compatibilidad con procesadores más viejos como el 386. Físicamente su conector es similar al tipo MCA, 112 contactos en dos filas de 56 donde se ubican 32 bits de datos, 30 líneas de direcciones, suficientes para direccionar 4 GB de memoria RAM.

La necesidad de "buferear" las señales de control, datos y direcciones siempre ha sido un compromiso velocidad-cantidad de extensiones del BUS. Los diseñadores de PC pueden aumentar el número de slots, agregando pases de buffer, pero sacrificando la velocidad de los mismos. No es el caso de VESA, sin embargo Ud. Habrá notado que no hay una cantidad mayor de tres buses locales en las tarjetas y esto se debe a una causa. Al aumentar el número de conectores aumenta la capacidad de la línea cuyos valores llegan a ser críticos al incrementar la frecuencia. El estándar VL-BUS recomienda no más de tres buses locales en sistemas de 33 MHz. No obstante, ello es suficiente para acomodar su tarjeta de video, su controlador de Disco Duro y su tarjeta de Red.

A diferencia de MCA la configuración del VESA no es automática. Se ha dejado libre a cada fabricante de tarjetas para escoger su propia configuración ya sea usando "jumpers", "switch" o mediante la configuración software EEPROM. El BUS en teoría es invisible al software; no requiere de drivers para tomar las ventajas de la alta velocidad.

Características de este bus

Elementos de Arquitectura y Seguridad Informática

VESA diseñó tres standard físicos para las tarjetas madres VL Bus: uno para ISA, otro para MCA y otro para EISA. Las tarjetas VL Bus incluyen (aunque no obligatoriamente) dos conectores, uno para el VL Bus y el otro para el bus tradicional. Los periféricos VL Bus toman los recursos de otros buses (interrupciones, control de DMA, etc.) de los cuales no está provisto el VL Bus. El VL Bus incluye solamente en el mismo la interrupción de hardware IRQ9.

VL Bus permite la operación de bus mastering utilizando la capacidad construida dentro del 486, pero usa señalización ligeramente diferente.

Cuando el bus master quiere tomar el control del bus, él envía una señal especial específica (LRQ(x)-pin A50) al sistema principal. El puede tomar el control cuando recibe la señal de confirmación (LGNT(x)-pin A52) del sistema principal. A diferencia del MCA o el EISA las especificaciones el VL Bus no establece las prioridades de los dispositivos de bus mastering. Las peticiones de arbitraje para usar el bus se deja a la tarjeta madre y a las peticiones de sus diseñadores. VL Bus soporta hasta tres bus master por subsistemas. La configuración automática no es parte de la especificación del VL Bus . El VL Bus es invisible al software. La configuración de los productos VL Bus es igual a los ISA usando switches.

La más importante innovación inherente al VL Bus es una alta velocidad de operación. En realidad, la alta velocidad del VL Bus viene dada por su burst mode que consiste en: un ciclo sencillo de direccionamiento seguido por cuatros ciclos de datos (5 ciclos para transferir cuatro palabras dobles). Para otras (non-burst) transferencias VL Bus requiere de los mismos dos ciclos (dirección y luego datos) para cada transferencia como hacen otros buses.

PCI

Intel Corp. Introdujo su variante de BUS local, llamado Peripheral Component Interconnect (PCI) en julio de 1992. Su retraso en establecerse en el mercado se debió en gran medida al silencio por parte de sus creadores en cuanto al pinout de su conector, frenando indiscutiblemente la fabricación de tarjetas para el mismo. Esta situación fue remediada un año después con la versión mejorada de PCI 2.0 y que además ampliaba el ancho de BUS a 64 bits dejándolo listo para la nueva generación de procesadores como el Pentium.

Es sin duda, la mayor virtud de PCI, acomodar en su estructura todo lo más avanzado en el campo del diseño hoy en día. Así PCI permite el uso de multiprocesamiento y a su vez prevé el uso de periféricos de alto nivel de prestaciones, soporta " arbitraje del BUS" (esto es gobernar cada una de las interrupciones de acuerdo con las prioridades de su solicitante), posee su propio lenguaje de comandos y caché de los datos transferidos.

Más allá de estas bondades, lo que parece más prioritario es la gran independencia que posee PCI del procesador, lo que lo hace virtualmente un estándar independiente de la familia de procesadores que posea la tarjeta madre. Otro

beneficio de PCI consiste en su fácil conexión con el sistema. Es decir PCI elimina lo que se conoce como "glue logic" que no es más que todos los integrados intermedios que unen a los grandes circuitos VLSI. Esto facilita enormemente la fabricación de las tarjetas madres: menos integrados en una tarjeta implica menos integrados a fallar, por supuesto, menos integrados a pagar.

A diferencia de VESA, el BUS local de Intel puede coexistir junto con los estándares actuales de BUS de forma independiente o servir de complemento de éstos en un mismo sistema. Su conector es de 124 pines (188 para la variante de 64 bits). Al igual que VESA y a pesar de la ubicación de las señales en el conector y los detalles de fabricación que brinda Intel con la norma, no más de tres buses deben estar presentes en un sistema. Los sistemas actuales llegan a tener más de tres buses PCI.

A pesar de lograr prestaciones al nivel de BUS local, PCI realmente se halla a un paso del procesador. En lugar de poseer su propio reloj el mismo está atado al reloj del procesador y su circuitería adyacente, de forma que está plenamente sincronizado con todo el sistema. Por otro lado el BUS puede pasar a estado de letargo y está preparado para trabajar no sólo a 5V si no a 3.3V para diseños de bajo consumo.

Como MCA y EISA, PCI permite configuraciones sin la necesidad de jumpers o switch y cada tarjeta debe incluir un registro donde se almacene la información de la misma. En otras palabras PCI se adviene mejor a la tecnología "Plug & Play".

Realmente la importancia de los buses locales es su alta velocidad y su elevado nivel de prestaciones. Tanto uno como el otro están pensados para dejar muy atrás la barrera de los 8 Mbs de ISA y en teoría alcanzar 400 Mbs. Estos picos de transferencia que le atribuyen a los buses locales solo se logran usando modos de transferencia de alta velocidad como el "bursts mode" en el cual a un ciclo único de acceso le siguen varios ciclos consecutivos de transferencia de datos en localizaciones adyacentes. Estos tipos de ciclos son los únicos capaces de aprovechar en toda su magnitud la potencialidad de los buses locales.

Ahora para ciclos normales ambas especificaciones requieren de los mismos dos ciclos para transferencias e incluso la inserción de estados de espera para velocidades por encima de los 33 MHz. Es por ello, que en la práctica la presencia de estos buses se pueden catalogar como un aumento de un 30 % en las prestaciones de su sistema. Incluso en ambientes gráficos como Windows, tal vez una tarjeta aceleradora de video puede lograr niveles similares e incluso superiores que una BUS local. Por otro lado es bueno recordar que el BUS sigue siendo un intermediario entre su sistema y los siempre comparativamente lentos periféricos. Así vemos que la presencia, por ejemplo, de un Disco Duro rápido agradece enormemente el aumento de la velocidad de trabajo.

Finalmente podemos decir que el Bus PCI de INTEL se ha impuesto debido a su diseño y prestaciones.

Características físicas

Elementos de Arquitectura y Seguridad Informática

El diseño del bus PCI prevé un máximo de tres conectores PCI. Como ocurre con el bus VESA esta limitante viene dada por la alta frecuencia de operación del bus. Más conectores incrementarían la capacitancia del bus y haría menos real la operación a máxima velocidad.

Para obtener operaciones reales a altas velocidades sin necesidad de terminaciones (como requiere el bus SCSI), Intel seleccionó el sistema de señalización reflejada en vez del sistema de señalización directa. Para activar una señal del bus, los dispositivos elevan (o bajan) la señal en el bus a la mitad del nivel de activación requerida. Como con cualquier otro bus, las señales de alta frecuencia se propagan por las líneas del bus y son reflejadas por los extremos de los conductores sin terminaciones. La señal reflejada se combina con la señal original doblando su valor hasta el voltaje de activación requerido.

El interface PCI básico requiere solo de 47 conexiones discretas por tarjetas esclavas (o dispositivos) con dos o más tarjetas bus masters. Para acomodar señales múltiples de alimentación, señales de tierra y espacios en blanco en la llave del conector para una correcta inserción, físicamente el conector de 32 bit PCI incluye 124 pines. La 64 bit implementación del PCI usa 188 pines en el conector.

Ciclos de transferencias de datos

Aunque el número de conexiones suena alto, Intel realmente tiene su mecanismo para mantener el número de pines manejable.

Así tenemos, que las señales de direccionamiento y de datos del PCI son multiplexadas en el tiempo en los mismos 32 pines, es decir que señales de direcciones y de datos comparten las mismas conexiones del bus (AD00 hasta AD31). En un ciclo del reloj, estas líneas llevan los valores de direcciones de donde tomarán o llevarán la información. En el siguiente ciclo, las mismas líneas transportan los valores del dato.

Este ciclo de direcciones/datos no reduce la velocidad del bus. PCI tiene su modo burst propio que elimina la necesidad de la alteración entre los ciclos de direcciones y datos. Durante la transferencia en el modo burst a un ciclo de dirección sencillo lo siguen ciclos múltiples de datos de acceso secuencial a localizaciones de memoria, limitado solamente por las necesidades de otros dispositivos a usar el bus y de otras funciones (como refrescamiento de memoria).

PCI logra la multiplexación usando la señal del bus llamada Cycle Frame (FRAME#). La aparición de esta señal indica que en el bus está la dirección válida. Después, esta señal se mantiene activa durante la transferencia de datos. Este modo en el PCI es equivalente al modo Streaming Data del MCA y el EISA, donde si esta señal (FRAME#) se mantiene activa durante varios ciclos múltiples de datos, el modo burst ocurre.

Este modo burst logra 132 MB/seg para el diseño 32 bit PCI(para la 64 bit extensión, PCI logra 264 MB/seg).

También, las señales Byte Enable (C/BE0# hasta C/BE3#) son usadas para indicar cual de los cuatro bloques del PCI de 32 bit contiene el dato válido. En los 64 bits sistemas, otras cuatro señales (C/BE4# hasta C/BE7#) indican los byte adicionales activos. Para acomodar dispositivos que no pueden operar a la máxima velocidad del bus PCI, el diseño incorpora tres nuevas señales de control : Initiator Ready(IRDY# del pin B35), Target Ready (TRDY# del pin A36) y Stop (Stop# del pin A38). Target Ready cuando es activada, indica que el dispositivo del bus está listo para suministrar el dato durante el ciclo de lectura o aceptarlo durante el ciclo de escritura. Cuando Initiator Ready es activada indica que el bus master está listo para completar la transacción. La señal Stop es enviada por el dispositivo fuente al master para detener la transacción actual.

Señales de integridad de datos

Las especificaciones del PCI permiten realizar el chequeo de paridad de los ciclos de dirección y de datos. Un bit (PAR) es usado para confirmar la paridad a través de las 32 líneas de direcciones/datos y de las cuatro señales Byte Enable. Una segunda señal de paridad es usada en la 64 bit implementación.

Si es detectado error de paridad durante la transferencia de datos, el controlador del bus inserta la señal Parity Error (PERR#). Otra señal, System Error (SERR#) señala paridad de dirección y otros errores.

Bus mastering y Arbitraje

El diseño básico PCI soporta el arbitraje de bus mastering como otros buses de expansión avanzados, pero el PCI tiene su propio lenguaje de comando de bus y soporta memoria cache secundaria.

A diferencia del MCA y el EISA en los cuales las señales de control del arbitraje están colocadas en el bus juntas, en el PCI cada tarjeta PCI tiene su propio slot, para pedir y recibir confirmación del control del bus. Esto permite gran flexibilidad en la asignación de prioridades, incluso en el protocolo de arbitraje.

El bus mastering a través del bus PCI se logra con dos señales especiales Request (REQ#) y Grant (GNT#). El master inserta su señal Request cuando el quiere tomar el control del bus. En el retorno el Central Resource (nombre dado por Intel) envía la señal Grant al master para dar permiso a tomar el control. Cada dispositivo tiene sus propias señales dedicadas Request y Grant.

PCI incluye cuatro interrupciones activadas por nivel (INTA# hasta INTD# de los pines A6,B7,A7,B8) que permiten compartir interrupciones. La especificación no define que interrupción y como son compartidas. Incluso, la relación entre las cuatros señales es dejada al diseñador.

Evolución Bajo-Voltaje

Para acomodarse a las PC green de bajo voltaje PCI especifica dos tipos de conectores y tres regímenes diferentes del conector : 5-volt conector para los diseños de circuito que aún prevalecen, 3.3-volt conector para diseños de baja potencia, y la capacidad de combinar ambos conectores en una tarjeta sencilla de expansión para una transición suave entre los diseños. Una llave en los 5-volt del socket (bloqueando los pines 50 y 51) evitan la inserción de tarjetas de 3.3 volt.

Una llave en los 3.3 volt del socket, permite solo la inserción de tarjetas de 3.3 v (en los pines 12 y13). Las tarjetas capaces de aceptar los dos regímenes de voltaje tienen slots en ambos lados.

Setup

Como con el MCA y el EISA contempla configuración sin la necesidad de establecer jumpers.o DIP switches.

Bajo la especificación de PCI, las tarjetas de expansión incluyen registros, que almacenan la información de la configuración que es usada para establecer el setup automáticamente.

Una señal especial Initialization Device Select (IDSEL), dedicada a cada slot es usada para activar la configuración leída y escribir operaciones.

Bus PCMCIA

PCMCIA (Personal Computer Memory Card International Association; Asociación Internacional de Tarjetas de Memoria para Ordenadores Personales) es una asociación con más de 575 fabricantes que ha creado un estándar para tarjetas de entrada/salida de pequeño tamaño (como una tarjeta de crédito), tales como discos duros, módem, fax, conectores SCSI. Por tanto, la especificación PCMCIA está al mismo nivel que las ranuras de expansión ISA, EISA o MCA y con ellas ha de luchar. En realidad, todavía no existe una confrontación directa entre ellas, pues por ahora el estándar PCMCIA se ha centrado únicamente en los portátiles y no en los ordenadores de sobremesa, pero también se podría utilizar en dichos ordenadores de sobremesa.

Cuando se creó la asociación PCMCIA, en 1989, su objetivo era crear estándares hardware y software para la conexión entre tarjetas de memoria removibles y sus receptáculos. En esta época, la PCMCIA y su especificación sólo se ocupaban de tarjetas de memoria removibles de uso general. En los años posteriores PCMCIA ha incluido definiciones para todos los periféricos que se conectan habitualmente en un PC.

El propósito final de PCMCIA es permitir al usuario conectar y desconectar fácilmente las tarjetas de su portátil, así como cambiar las funciones y características en un instante, sin importar el fabricante y el tipo de portátil. Las tarjetas PCMCIA actuales incluyen tarjetas de memoria (SRAM, DRAM, ROM, memoria flash, etc.), discos duros, dispositivos de comunicaciones (módem, fax, comunicación inalámbrica), adaptadores LAN (Ethernet y Token Ring), conectadores SCSI, tarjetas de sonido, puertos serie RS-232-C, etc.

Los beneficios de las Tarjetas PCMCIA

- Tamaño pequeño.
- Inserción de conexión sencilla.
- Alto rendimiento.
- Independencia del host.
- Tecnología de Ejecución en el Lugar (XIP).
- Intercambio Rápido.
- La tecnología PCMCIA coloca a los poderosos periféricos en la palma de su mano literalmente.
- Estas tarjetas clasificadas son un enlace para las computadoras portátiles con el mundo exterior.

Estándares PCMCIA

La norma PCMCIA especifica un dispositivo removible que mide 2.126" x 3.37" (5.4 x 8.6 cm). Básicamente, ese es el tamaño de tres tarjetas de créditos amontonadas. Las tarjetas PCMCIA tienen asignaciones de 68 números de identificación personal, e interconexión con buses tanto de 8 como de 16 bits. También soportan puerto físico de hasta 64 MB de memoria.

Las tarjetas PCMCIA le dan una capacidad de expansión universal para laptops, y pueden soportar una variedad de funciones incluyendo fax en radio y en líneas de cables y capacidades de módem, almacenamiento masivo y extensión de memoria.

Ranuras PCMCIA

Hay tres tipos de ranuras PCMCIA, y pronto llegará una cuarta. Estas ranuras son identificadas por el espesor de las tarjetas que se adapta en ellas. Todos los tipos son compatibles inversamente.

Tarjetas del Tipo I: Son de 3.3 mm de espesor. Son usadas principalmente en Asistentes Personales Digitales (PDAs) y dispositivos portátiles como RAM, FLASH memory, memoria de sólo lectura electrónicamente programable (EEPROM), y memoria programable una vez (OTP).

Elementos de Arquitectura y Seguridad Informática

Tarjetas del Tipo II: Son de 5 mm de espesor y tienen totalmente capacidad I/O. Las puede usar para ampliación de memoria o para aspectos I/O en modems, conexiones de red y comunicaciones.

Tarjetas del Tipo III: Miden 10.5 mm de espesor. Están diseñadas principalmente para unidades duras removibles y dispositivos de radiocomunicación que requieren un mayor tamaño. También pueden ser usadas para almacenamiento de memoria.

Tarjetas del Tipo IV: Aún no han sido ratificadas por el consorcio PCMCIA. El tamaño exacto se espera que sea de 18 mm de espesor. Las tarjetas del tipo IV se usarán para unidades duras de gran capacidad.

¿ Cómo trabajan las tarjetas PCMCIA?

La norma PCMCIA define seis estándares fundamentales de hardware y software: para la tarjeta misma, la interconexión conector/adaptador, servicios de conector, servicios de tarjeta, la estructura de información de tarjeta (CIS) y el software.

La tarjeta PCMCIA se conecta en un conector/adaptador host en el tablero matriz de la computadora o conectado a su luz de expansión.

El lado del conector tiene la interconexión estándar de 68 agujas para la tarjeta. El lado adaptador traduce las señales de interconexión PCMCIA para comparar los estándares del bus de la computadora.

Socket Services (“Servicios de Conector”) se refiere a la interconexión de software entre la tarjeta, el conector y el adaptador al bus de la computadora. La interconexión estándar de los Servicios de Conector, es lo que permite el uso de cualquier tarjeta PCMCIA en cualquier PC equipada con un conector/adaptador.

La interface programadora para PCMCIA es llamado servicios de tarjeta. Envía las señales para enlazar los servicios de conector al sistema operador de PCs y hardware. Los servicios de tarjetas pueden ser ejecutados, ya sea como un programa de instrucciones periféricas, o en el sistema operacional como lo es IBM DOS 6.0. La estructura de información de tarjeta (CIS) contiene información sobre las funciones de la tarjeta, su tamaño, sus necesidades eléctricas, etc. Al ser insertada la tarjeta, pasa esa información identificadora al sistema host. El sistema software lee los datos CIS en la inserción, instala los circuitos de instrucciones adecuados, notifica los recursos de sistema relevantes y pone las iniciales a la tarjeta para que esté disponible para ser usada por el host.

Las tarjetas PCMCIA son dispositivos móviles en los que no sólo es importante un tamaño pequeño y un peso ligero, sino que existen otros factores fundamentales como la potencia consumida y las técnicas empleadas para proteger un producto móvil. Y en estas cuestiones las tarjetas PCMCIA responden a la perfección. La mayoría de las tarjetas PCMCIA se pueden desconectar cuando no están en uso, de forma que consuman apenas 0.1 watios. Casi todas las tarjetas de memoria flash (memoria grabable y no volátil) son dispositivos de 12 voltios, pero actualmente

están apareciendo tarjetas de 5 voltios que reducirán dramáticamente la potencia consumida.

Las tarjetas PCMCIA también son resistentes a los problemas inherentes a los dispositivos móviles. Si se cae una tarjeta PCMCIA al suelo, sufrirá pocos o ningún daño. Por ejemplo, la mayoría de los discos duros PCMCIA pueden sufrir golpes de cientos de g's, mientras que los discos duros normales apenas aguantan un choque de 100g.

Características físicas

Todos los tipos de PC Card usan el mismo conector de 68 pines donde los contactos están ordenados en dos hileras paralelas de 34 pines. Las tarjetas tienen medidas standard, así como está estandarizado la posición del switch de protección de escritura (si lo tiene) y de la batería (si la necesita). La batería se recomienda colocarla con el terminal positivo hacia fuera. Para la correcta alimentación de las tarjetas, las conexiones de alimentación y de tierra son más largas (3.6 mm) que el resto de las señales (3.2 mm). La interface para tarjeta de memoria se convirtió en ranura PCMCIA tipol. Una ranura tipol es de 3.3 milímetros de espesor, con un conector para 68 patas. La mayor parte de las tarjetas tipo I, son de memoria, ya sea RAM normal o tarjetas de memoria especiales que incluyen un programa(Ej: lotus 1-2-3 y Word Perfect existen disponibles en este tipo de tarjetas). La necesidad de un módem interno, condujo a la ranura tipo II. Al desarrollar la ranura tipo II, se desarrollo un componente standard para programas llamado Card Services y Socket Services (Servicios de Tarjetas y Servicios de Receptáculo). Las tarjetas tipo II pueden diseñarse para funcionar como un objeto que se coloca directamente en espacio de direcciones de la memoria de la PC.

Si compra un programa en una tarjeta tipo I como el caso citado de WP, la PC tendría que copiar los datos de la tarjeta tipo I a la memoria de la PC antes de poder correr el programa contenido en la tarjeta. Eso toma tiempo y usa algo de la memoria de la PC, con los de tipo II, no es necesario, con lo cual el arranque es mas rápido y aumenta la cantidad de memoria libre disponible.

Las tarjetas tipo II son de 5 milímetros de grueso, lo cual les da más espacio para circuitos complejos. Las tarjetas tipo I trabajan en ranuras tipo II. Más recientemente PCMCIA ha definido una especificación tipo III, suficientemente flexible para dar soporte a discos duros removibles. La principal novedad de los tipos III es que es mucho más gruesa, las tarjetas tipo III pueden ser de 10.5 mm de grueso. Al comprar tarjetas tipo III asegúrese de que lo que compre se apega al standard, cuídese de discos duros mal llamados tipo III que tenían 13 mm de espesor.

PCMCIA da soporte a la capacidad de rutas y de instalar tarjetas PCMCIA al vuelo. Todos los demás busés requieren que se apague la computadora antes de instalar o quitar una tarjeta, por lo contrario, PCMCIA da soporte a cambios andando. La computadora da soporte a esta capacidad con dos niveles de programas de soporte.

Elementos de Arquitectura y Seguridad Informática

Señales y Operaciones.

El standard del conector PCMCIA 2.0 permite dos variaciones de PC cards: solo de memoria (las cuales conforman esencialmente la versión 1.0 del standard) y tarjetas I/O. Cuatro señales de la tarjeta de memoria están definidas diferente para las tarjetas I/O (pines 16, 33, 62, 63); tres señales de tarjeta de memoria están modificadas para funciones I/O y tres pines reservados en tarjetas de memoria son usados por tarjetas I/O.

En operaciones de memoria, 2 señales Card Enable (pin 7 y 42) establece el ancho del bus.

Para direccionar 64 Mb de datos se usan 26 líneas de direcciones.

Las áreas de memoria son independientes para cada tarjeta, esto significa que cada tarjeta puede definir su propio rango de direcciones como su Common Memory.

En adición con la Common Memory, cada tarjeta tiene un segundo espacio de direcciones dedicada a Attribute Memory que contiene la información del setup de las tarjetas.

Activando la señal Register Select (pin 61) se conmuta las 26 líneas de direcciones usadas para direccionar la Common Memory, para localizaciones específicas en Attribute Memory.

Para abrir o cerrar el acceso al dato leído desde una PC card, el micro principal activa la señal de la tarjeta Output Enable Line (pin 9). La línea Ready /Busy (pin 16) en tarjetas de memorias indican cuando ellas están ocupadas procesando y no pueden aceptar operaciones de transferencia de datos. Este mismo pin es usado en tarjetas I/O para hacer peticiones de interrupciones al sistema principal. Durante el setup, las tarjetas de I/O pueden redefinir el pin 16 como función Ready /Busy.

El pin Write Protec (pin 33) transmite el estado del switch de protección de escritura al sistema principal. En tarjetas de I/O este pin indica que el puerto de I/O dado tiene 16 bit de ancho. Los pines 62 y 63 en tarjetas de memoria muestran el estado de la batería. El pin 63 indica el estado de la batería: cuando esta activada, la batería está en buenas condiciones; cuando no está activado, indica que la batería necesita ser reemplazada. El pin 62 indica si el nivel de batería es suficiente para mantener la tarjeta de memoria sin errores. Cuando no está activada indica que la integridad de la tarjeta está comprometida.

Los pines 18 y 52 proveen valores de voltaje superiores cuando se necesitan para reprogramar los chips de la Eprom memory.

Las mismas 26 líneas usadas para direcciones al Common y Attribute Memory, sirven como direcciones de selección de puertos en la tarjeta I/O. Dos pines I/O read (44) y I/O write (45) indican que los pines de direcciones son usados para identificar puertos y las operaciones de lectura o de escritura.

La especificación PCMCIA requiere que todos los PC card sean capaces de generar las interrupciones activadas por marginalidad y las interrupciones activadas por nivel. Cada tarjeta se conforma a los requerimientos del sistema principal.

Una línea de salida de audio es disponible en la tarjeta I/O. Esta conexión no usa sonidos de alta calidad.

PCMCIA 2.0 contempla también el uso de PC card que opera al estándar TTL-5volt y el nivel de voltaje reducido de 3,3 v.

Interface de software

Para unir las PC cards con el micro de la PC de arquitectura Intel, PCMCIA ha definido un interface de software llamado Socket Services. Se llama a la interrupción 1A (la cual el Socket Services comparte con el CMOS time-of -day clock) y el software puede acceder a las características de la PC card sin conocimiento específico del hardware subrayado. En otras palabras, el Socket Services hace el acceso al hardware independiente de la PC cards.

En realidad, Socket Services están diseñados de forma tal que pueden ser contruidos dentro del BIOS de la PC. Socket Services puede ser también implementado en forma de controlador de dispositivos, por lo que esa funcionalidad de PCMCIA puede ser adicionada a las PC existentes.

Usando Socket Services el micro principal puede direccionar directamente memoria o registros. Alternativamente, a través llamadas de funciones de Socket Services pueden ser leídos o escritos uno o múltiples bytes.

En septiembre de 1992, PCMCIA aprobó un Standard de Services Cards, que define un programa de interface para acceder a las PC cards. Este standard establece una serie de llamadas de programas que unen a estos Socket Services independiente del sistema operativo principal.

Setup Automático

PCMCIA desarrolló un sistema contenido en el mismo. a través del cual la información básica de la tarjeta del Setup puede ser pasada al sistema principal sin hacer caso de la estructura del dato en las tarjetas de almacenaje o del sistema operativo del sistema principal.

Conocida como Estructura de Identificación de Tarjeta (Card Identification Structure - CIS), el sistema de configuración de PCMCIA trabaja a través de una sucesión de estratos compatibles para establecer la unión necesaria entre las PC cards y el sistema principal.

Solamente el primer estrato, Estrato de Compatibilidad Básica (Basic Compatibility Layer) es obligatorio bajo PCMCIA. Este estrato indica como es organizado el almacenaje en la tarjeta. Solo dos tipos de información son relevantes: las estructuras del dato usadas por el mismo estrato e información standard y física de

Elementos de Arquitectura y Seguridad Informática

dispositivos tales como: número de cabezas, cilindros, sectores del disco físico o emulado.

El siguiente estrato conocido como: Estrato del Formato del Dato Grabado (Data Recording Format Layer), como es organizado el dato almacenado en el nivel de bloque. Cuatro formatos de datos son soportados: bloques no chequeados, bloques con corrección del checksum, bloques con chequeo de error de redundancia cíclica y datos que no se corresponden con la organización del disco (Ej : el acceso aleatorio al dato, tal como es permitido para la memoria).

El tercer CIS es el Estrato de Organización del Dato (Data Organization Layer), y especifica como la información es lógicamente organizada en la tarjeta, se especifica el formato del sistema operativo para conformar el dato. PCMCIA reconoce cuatro posibilidades: DOS, Microsoft's Flash File System for Flash Ram, ejecución propia del PCMCIA en (o XIP) Rom imagen, y organización de aplicación específica. Flash File System es un sistema operativo especialmente diseñado para restringir la memoria Flash. Esto minimiza la rescritura de áreas específicas de memoria para extender la vida límite del medio y permitir la actualización rápida de bloques de escritura requeridos.

La ejecución propia en (XIP) Rom imagen permite al programa de códigos en memoria ROM ejecutarse sin ser cargado en la memoria del sistema principal (RAM). La organización de la aplicación específica permite a los creadores de tarjetas desarrollar una organización única de los datos a sus productos e implementar las características especiales.

El cuarto estrato CIS a un sistema standard específico que se conforma con un ambiente operativo particular Ej : el standard XIP define como los códigos de programas en tarjetas ROM van a ser leídos y ejecutados.

La información del Setup para todos estos estratos es almacenada en un área reservada de la tarjeta llamada Attribute Memory. Esta área está separada del área de almacenaje común de las tarjetas llamado Common Memory. La información del CIS es estructurada como cadenas unidas de bloques de datos llamados tuples que pueden ser de hasta 128 bytes. Para dar a todos los sistemas un punto común de partida para buscar los datos CIS, el primer tuple se localiza en la primera dirección del Attribute Memory. Como el sistema CIS puede trabajar en cualquier PC u otro sistema principal, la tarjeta asume que la memoria puede ser accedida solamente en anchos de byte. Los primeros dos bytes de cada tuple están estrictamente definidos. El primer byte codifica la función del tuple y los parámetros que el describe. El segundo byte se une con el siguiente tuple de la cadena (si lo hay), él especifica el número de bytes del dato en el tuple.

La especificación PCMCIA 2.0 define las opciones disponibles para varios tuples comunes. Los diseñadores en PC cards están libres para adicionar sus propios tuples para almacenar información para tarjetas que contienen características propias.

Comparación de PCMCIA con otros buses

Espacio de direcciones de memoria: PCMCIA da soporte a 64-MB de posibles direcciones, esto se debe a que el bus usa 26 bits para direccionar y 2^{26} elevado a la potencia 26 es aproximadamente 64 millones.

Bus mastering: PCMCIA no da soporte a bus mastering ni a DMA.

Configuración Conector y Operador: PCMCIA permite- requiere que las configuraciones de equipo se hagan con programas en virtud de las pequeñas dimensiones físicas de las tarjetas PCMCIA, nunca se verán presentes Switches ni puertas en ella.

Número Posible de Ranuras PCMCIA es un solo Sistema: La mayor parte de los otros buses no dan soporte a más de 16 ranuras. PCMCIA teóricamente puede dar soporte a 4,080 ranuras PCMCIA en una PC.

Ruta de Datos: La ruta de datos de PCMCIA es de solo 16 bits.

Velocidad: PCMCIA esta limitado a una velocidad de reloj de 33 Mhz, el tamaño pequeño de las tarjetas PCMCIA, a su pequeño consumo de energía hace que el nuevo bus sea muy atractivo, no únicamente para Laptop, sino para las llamadas PC "Verdes" diseñadas para consumir tan poca energía como sea posible. Por esta razón, PCMCIA puede convertirse en una norma importante de computadoras de escritorio así como portátiles Laptop.

BUS ATA/EIDE

Es el bus para almacenamiento de información. Permite añadir un máximo de 4 dispositivos, aunque nominalmente puede alcanzar velocidades de 16.7 Mbps solo se logra alrededor de la mitad. Soporta discos superiores a 528 Mbyte siendo una versión superior del antiguo bus IDE estándar, pudiendo llegar hasta 8,4 Gbyte.

En los sistemas actuales esta interface viene implementada en el M/B y con características como:

- Soporte Bus Master para dispositivos IDE
- Soporte Ultra DMA/33

En el caso de soporte Bus Master, significa un conjunto de chips integrados en el M/B y que permiten el control de las transferencias entre la memoria y los dispositivos IDE sin la intervención del procesador. Algo que se lograba en muchos de los buses antes mencionados con adaptadores (tarjetas) que se configuraban sobre las mismas.

El soporte Ultra DMA/33 es la nueva especificación en la relación de transferencia de datos de los discos IDE.

La tabla siguiente muestra la diferencia entre los distintos modos de transferencia implementadas por esta interface:

Tabla II-9

Interface	Modo	Transferencia
PIO	0	3,3 MB/s
PIO	1	5,2 MB/s
PIO	2	8,3 MB/s
PIO	3	11,1 MB/s
PIO	4	16,6 MB/s
DMA	0	4,16 MB/s
DMA	1	13,3 MB/s
DMA	2	16,6 MB/s
DMA/33		33 MB/s

BUS SCSI

Los adaptadores SCSI mejoran prestaciones llevando parte del trabajo fuera del CPU. Hoy en día la mayoría de estos se ajustan a las especificaciones SCSI-2.

La totalidad de los CDROM, Scanners y arreglos de discos (RAID) operan exclusivamente con interfaces SCSI. Si lo que necesita es mayor velocidad, mayor capacidad en disco o se tiene la idea de conectar varios dispositivos SCSI es la opción.

Variantes SCSI

- Fast – SCSI: Canal de datos de 8 bits. Transferencia de 10 Mbps.
- Fast – Wide SCSI-2: Ofrece 20 Mbps con canal de datos de 16 bits.
- Ultra Wide SCSI-3: Transferencia de 40 Mbps.

IEEE 1394 (fire ware): descrita anteriormente, tecnología serie SCSI. Puede lograr hasta 400 Mbps.

Nuevos Buses

Desde hace algún tiempo han ido apareciendo especificaciones de nuevos buses que poco a poco se irán añadiendo a la configuración base de cualquier ordenador compatible PC. Básicamente se trata de buses que intentan mejorar tanto el rendimiento del ordenador y de los periféricos que a él se conectan como facilitar al

usuario la conexión y configuración de dispositivos, ya que todos los nuevos buses se basan en la filosofía del estándar Plug & Play.

Los nuevos buses los podemos dividir atendiendo a si están creados para la conexión de dispositivos internos o externos. Por un lado AGP está destinado, evidentemente, sólo a la conexión de dispositivos internos, ya que su única función es proporcionar un conector para tarjetas gráficas. USB está diseñado para la conexión de dispositivos externos que no necesitan un ancho de banda demasiado elevado, con una tasa de transferencia máxima de 12 Mbits por segundo. Por último, el bus IEEE 1394 está desarrollado de tal forma que puede acomodar tanto dispositivos internos, como por ejemplo discos duros, como externos (por ejemplo una cámara de vídeo digital). Debido a la elevada velocidad de transferencia del bus 1394 (200 Mbits por segundo), este bus podría llegar a sustituir incluso al bus SCSI para la conexión de dispositivos de almacenamiento.

AGP

Este nuevo bus, destinado a la conexión de tarjetas gráficas equipadas con aceleración 3D por hardware, estará presente en todas las nuevas máquinas Pentium II basadas en el chipset 440LX, así como en los sucesores de este, y en algunas placas base para Pentium que usen el conjunto de chips Apollo VP3 desarrollado por VIA Technologies. Básicamente este bus es una evolución del bus PCI adaptado especialmente a las necesidades de los productos hardware de aceleración 3D.

La principal función del bus AGP es proporcionar un medio de alta velocidad a través del cual el procesador gráfico de una tarjeta aceleradora 3D pueda acceder de una manera lo más rápida posible a la memoria RAM del sistema.

De esta forma las imágenes que se aplican como textura a los polígonos tridimensionales generados por la tarjeta gráfica pueden almacenarse en la memoria de la placa base, y no en la RAM de la tarjeta gráfica. De esta forma es posible almacenar un mayor número de texturas o texturas de mayor calidad, lo cual redundará en la posibilidad de crear aplicaciones 3D mucho más realistas.

En lugar de funcionar a 33 MHz como el bus PCI, AGP puede trabajar en dos modos distintos dependiendo del soporte ofrecido por la tarjeta gráfica: modo x1 y modo x2. En el modo x1 el acelerador 3D puede acceder a la RAM del sistema a una velocidad de 66 MHz, mientras que en el modo x2 dicha velocidad asciende hasta 133 MHz. AGP es un bus con una anchura de 32 bits, por lo que con la máxima velocidad actual de 133 MHz es posible alcanzar una velocidad de transferencia máxima superior a los 500 MB por segundo.

Mediante el uso de líneas de control suplementarias una tarjeta 3D puede enviar varias peticiones de lectura, las cuales serán satisfechas a medida que el conjunto de chips de la placa base pueda cumplimentarlas. Esta funcionalidad hace posible que el acelerador 3D pueda continuar enviando peticiones de lectura sin que aún no se hayan completado peticiones previas.

Elementos de Arquitectura y Seguridad Informática

AGP necesita un soporte software especial, ya que en los sistemas operativos actuales es necesario instalar un controlador de dispositivo que gestione la tabla GART (Graphics Address Remapping Table) mediante la que se convierten las direcciones de memoria enviadas por el acelerador gráfico a través del bus AGP en direcciones de memoria física. Este mecanismo de conversión de direcciones es necesario debido a la fragmentación de memoria existentes en los sistemas operativos actuales, la cual se debe a los mecanismos de paginación y memoria virtual que se emplean en la actualidad.

Por otra parte para aprovechar AGP es preciso que las aplicaciones lo tengan en cuenta, de forma que se indique al sistema que una textura debe almacenarse en memoria no local, es decir, en la memoria del sistema en lugar de en la RAM de la tarjeta gráfica. Mediante la serie de APIs englobadas bajo DirectX 5 es posible tener acceso a todas estas funciones, por lo que sólo los programas que usen dichas API podrán aprovechar las capacidades que ofrece AGP. Un punto a tener en cuenta es que cada fabricante de chipsets con soporte AGP debe proporcionar un controlador propio para gestionar la tabla GART, por lo que no es posible instalar el controlador de Intel en un sistema equipado con el conjunto de chips de VIA Technologies o viceversa.

USB

Este nuevo bus serie ofrece al usuario la posibilidad de conectar hasta 127 dispositivos de forma simultánea. En el cableado del bus se incluye la alimentación eléctrica necesaria para el funcionamiento de muchos tipos de periféricos que no realizan un consumo elevado, como pueden ser teclados, ratones, joysticks o escáneres. En algunos casos será preciso incluir una fuente de alimentación adicional, como sucede con algunos escáneres o con los monitores equipados con conexiones USB. La máxima velocidad de transferencia que se puede alcanzar con este bus es de 12 Mbits por segundo, lo que lo hace adecuado para la conexión de dispositivos que no precisen un elevado ancho de banda. Existe un modo para dispositivos lentos que permite la conexión de periféricos que transmitan datos a una velocidad de 1,2 Mbits por segundo.

Algunos tipos de dispositivos necesitan disponer de forma constante de un determinado ancho de banda, por lo que el bus USB dispone de modos en los que se garantiza a un determinado periférico un ancho de banda constante. Este tipo de funcionamiento será fundamental para utilizar algunos dispositivos de digitalización de vídeo para bus USB.

Otra cuestión importante es el soporte necesario por parte del sistema operativo. Actualmente la versión OSR2 de Windows 95 soporta USB, si bien habrá que esperar hasta que aparezca Windows 98 y Windows NT 5 para contar con un soporte totalmente integrado en la arquitectura del sistema operativo.

Desde que nació el PC de la mano de I.B.M., por motivos de compatibilidad, algunas de sus características han permanecido inalterables al paso del tiempo.

Conectores como el de la salida paralelo (o Centronics), la salida serie (RS-232) o el conector del teclado han sufrido muy pocas variaciones.

Si bien es cierto que estos conectores todavía hoy cumplen su función correctamente en casos como la conexión de un teclado, un ratón o un modem, se han quedado ya desfasados cuando tratamos de conectar dispositivos más rápidos como por ejemplo una cámara de video digital.

USB nace como un estándar de entrada/salida de velocidad media-alta que va a permitir conectar dispositivos que hasta ahora requerían de una tarjeta especial para sacarles todo el rendimiento, lo que ocasionaba un encarecimiento del producto, además de ser productos propietarios, que obligaban a adquirir una tarjeta para cada dispositivo.

Pero además, USB nos proporciona un único conector para solventar casi todos los problemas de comunicación con el exterior, pudiéndose formar una auténtica red de periféricos de hasta 127 elementos.



Figura II.7. Vista de un conector USB.

Mediante un par de conectores USB (Figura II.7) que ya hoy en día son estandar en todas las placas base, y en el espacio que hoy ocupa un sólo conector serie de 9 pines nos va a permitir conectar todos los dispositivos que tengamos, desde el teclado al modem, pasando por ratones, impresoras, altavoces, monitores, scanners, cámaras digitales, de

video, plotters, etc... sin necesidad de que nuestro PC disponga de un conector dedicado para cada uno de estos elementos, permitiendo ahorrar espacio y dinero.

Al igual que las tarjeta ISA tienden a desaparecer, todos los conectores anteriormente citados también desaparecerán de nuestro ordenador, eliminando además la necesidad de contar en la placa base o en una tarjeta de expansión los correspondientes controladores para dispositivos serie, paralelo, ratón PS/2, joystick, etc...

Como podeis ver, realmente es un estándar que es necesario para facilitarnos la vida, ya que además cuenta con la famosa característica PnP (Plug and Play) y la facilidad de conexión "en caliente", es decir, que se pueden conectar y desconectar los periféricos sin necesidad de reiniciar el ordenador.

Otras características que también deberemos saber son:

- Dos velocidades de acceso, una baja de 1,5 Mbps para dispositivos lentos como pueden ser joysticks o teclados y otra alta de 12 Mbps para los dispositivos que necesiten mayor ancho de banda.
- Topología en estrella, lo que implica la necesidad de dispositivos tipo "hub" que centralicen las conexiones, aunque en algunos dispositivos como teclados

Elementos de Arquitectura y Seguridad Informática

y monitores ya se implementa esta característica, lo que permite tener un sólo conector al PC, y desde estos dispositivos sacar conexiones adicionales. Por ejemplo en los teclados USB se suele implementar una conexión adicional para el ratón, o incluso otras para joystick, etc.. y en los monitores varias salidas para el modem, los altavoces, etc...

- Permite suministrar energía eléctrica a dispositivos que no tengan un alto consumo y que no estén a más de 5 metros, lo que elimina la necesidad de conectar dichos periféricos a la red eléctrica, con sus correspondientes fuentes de alimentación, como ahora ocurre por ejemplo con los modems externos.

IEEE 1394

Al igual que el bus USB, el bus 1394 es un bus serie que permite la conexión simultánea al ordenador de varios dispositivos. Las versiones actualmente disponibles soportan velocidades de transferencia máxima de 200 Mbits por segundo. Diversos fabricantes de hardware, como por ejemplo Adaptec, disponen de tarjetas para bus PCI que disponen de conectores para bus 1394.

La principal utilidad de este bus se centra en torno al uso de dispositivos que requieren un elevado ancho de banda, como puede ser el caso de las cámaras de video digital. Actualmente algunos fabricantes, como por ejemplo Sony, disponen de cámaras de video digital capaces de captar imágenes en movimiento, comprimirlas en tiempo real y enviar los datos a un ordenador al que se conectan a través del bus 1394.

Al igual que ocurre con el bus USB para usar dispositivos que se conecten a dicho bus es preciso contar con soporte del sistema operativo. Actualmente solo es posible obtener dicho soporte mediante controladores de dispositivo y APIs desarrolladas por los fabricantes de tarjetas adaptadoras. Adaptec dispone de placas y kits de desarrollo de software para las empresas y particulares interesados en desarrollar productos para bus IEEE 1394.

Memoria RAM y tiempos de acceso

Memoria de Acceso Aleatorio. (Random Access Memory, RAM).

En este tipo de memoria, el Microprocesador no tiene que leer o escribir a través de una larga cadena de datos, sino que puede hacerlo directamente en la localización que desee; esta razón es que se conocen como Memoria de Acceso Aleatorio. Existen varios tipos de memoria RAM dependiendo de la tecnología empleada en su fabricación:

Memoria RAM Dinámica (DRAM).

Memoria RAM Estática (SRAM).

A continuación analizaremos las características generales de cada uno de estos tipos

Memoria RAM estática (Static RAM, SRAM).

La RAM más sencilla es la llamada estática, cuyo diseño no tiene ninguna dificultad: Un integrado que guarda los datos pasivamente. Esta memoria se distingue con las siglas SRAM y tiene tres particularidades.

- Es potencialmente muy rápida (Alta velocidad de acceso).
- Es difícil construir integrados de alta capacidad.
- Alto costo de producción.

Comúnmente abreviada como **SRAM**. Este tipo de memoria se caracteriza por: No tratan de almacenar la carga, por tanto no tienen capacitores. Ellas operan como un interruptor o switch que potencialmente permite o detiene el flujo de electricidad. Estos interruptores, son materializados con transistores los cuales son alambrados como circuitos latch o biestables. Estos se caracterizan por almacenar un bit de información. Un gran número de estos flip-flops convenientemente miniaturizados y arreglados, conforman el chip de Memoria Estática. Debido al elemento digital que utilizan como almacenador no permiten chips con muy alta capacidad. La principal diferencia entre la memoria estática y dinámica es que la SRAM no necesita ser periódicamente refrescada y es notablemente más rápida. La principal semejanza es que ambas necesitan una fuente de corriente continua para mantener la información.

Instalación de la DRAM

Es necesario revisar en el manual las posibles combinaciones de memoria DRAM. Verificar en este si la tarjeta permite detectar automáticamente la cantidad de memoria instalada o si es necesario indicárselos mediante algunos *Jumpers* (en algunas tarjetas 486DX4/100 esto es necesario sobre todo aquellos que tienen bus local VLB).

Localizar correctamente los bancos de memoria, ya sea por el manual o por que lo indique la Tarjeta Madre en su superficie.

Recordar que las tarjetas madres con microprocesadores 486 necesitan al menos un SIMM de 32 bits (72 pines) y las que soportan Pentium necesitan dos como mínimo para cubrir el bus de datos de 64bits. Las tarjetas que aceptan DIMM solo necesitan uno para llenar el bus de datos puesto que los DIMM son de 64bits (128 pines).

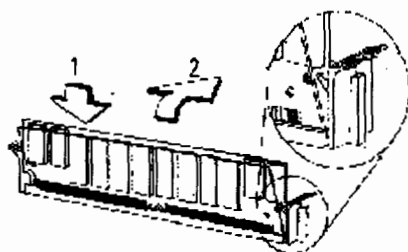


Figura II.8. Esquema donde se muestra la forma de conectar la memoria SIMM.

Para colocar los SIMM's de memorias observe los siguientes pasos (Figura II.8):

1. Coloque el SIMM en un ángulo de 45° en la base.
2. Suavemente empújelo hasta que entre correctamente y las presillas laterales lo mantengan en una posición vertical.
3. Sea cuidadoso cuando inserte o quite los SIMM's. Estos entran en una sola posición y forzarlos puede dañar la base, el SIMM's o ambos.

¿Pueden los DIMM SDRAM trabajar conjuntamente con los SIMM EDO/FPM?

Los SIMM EDO/FPM operan a 5V mientras que los SDRAM operan a 3.3V. Los diseños de las tarjetas madres actuales suministran voltajes de alimentación diferentes para los DIMM y los SIMM, pero interconectan sus buses de datos. Si se combinan los SIMM y los DIMM el sistema podría trabajar bien, sin embargo esto solo es temporal, al cabo de cierto tiempo la entrada de datos de 3.3V de los DIMM podrá ser dañada por la salida de datos de 5V de las memorias EDO/FPM. Por tanto es altamente recomendable NO mezclar los DIMM con los SIMM. Esto es solo posible hacerlo si su memoria SDRAM soporta tolerancia a los 5V (como las TI o Samsung), es decir si su memoria acepta señales de 5V con una alimentación de 3.3V entonces si es posible combinarlas.

Localización de la DRAM en la PC

Esta memoria es donde se almacenan los programas y sus datos. Incluye la memoria convencional, la memoria extendida, y podría incluir la memoria expandida, si esta existe.

Antiguamente las memorias se incorporaban al ordenador en circuitos integrados sueltos que se insertaban en bases. En la actualidad se distribuyen en módulos de **SIMM** (Single In-Line Memory Modules) o **DIMM** (Dual In-Line Memory Module) de memorias.

Estos módulos no son más que pequeñas tarjetas de circuito impreso sobre las que van montadas las pastillas de memoria DRAM, ocupan los bancos de memoria en la tarjeta madre y suministran hasta 128 MB de memoria del sistema.

Es importante destacar que los SIMM y los DIMM se diferencian por el número de líneas de datos que permiten, el número de pines y por el voltaje de alimentación.

Los SIMM de 30 pines fueron muy populares en los sistemas 386 y 486; para estos Microprocesadores el banco de memoria debía llenarse con al menos dos de estos módulos (386 y 486 SX) o con cuatro (486 DX/DX2/DX4) para cubrir enteramente el bus de datos.

En los sistemas 486 también se utilizaron los SIMM de 72 pines ampliamente. En este caso solo es necesario un módulo para llenar los 32 bits del bus de datos. Por último los sistemas que utilizan el Pentium como procesador soportan tanto SIMM como DIMM y necesitan 2 y 1 como mínimo, respectivamente.

Existen varios tipos de **SIMM** de memoria dependiendo de las características y organización lógica de los chips que emplean:

Por estas tres razones, es inviable utilizar SRAM como memoria principal de un ordenador, aunque puede usarse con otros fines como la memoria cache, que luego veremos.

Otro método para que el integrado de memoria recuerde los datos, es realizar un refrescamiento de los mismos cada cierto tiempo. Esto permite la construcción de memorias de gran capacidad a un costo mucho menor, pero, como contrapartida ese refrescamiento entorpece el acceso a la memoria, disminuyendo la velocidad. A estas memorias se les denomina dinámicas o DRAM y se utilizan habitualmente como memoria principal de un ordenador.

La Tabla II-10 muestra un resumen de estas características:

Tabla II-10

Tipo de módulo	Bus de datos	Números de pines	Voltaje	Tiempo de acceso	Capacidad típica (MB)	Tipo de memoria
SIMM	8 Bits	30	5 V	70/80 ns	1,4,8,16	DRAM
SIMM	32 Bits	72	5V	60/70 ns	4,8,16,32,64	FPM,EDO
DIMM	64 Bits	128	3.3V/5V	60/70 ns	16,32	EDO
DIMM	64 Bits	128	3.3V	10ns (100Mhz) 12ns (80Mhz) 15ns (66Mhz)	32,64	SDRAM

FPM RAM

Aunque hoy en día está obsoleta, la memoria FPM RAM es la que está instalada en muchos sistemas 486 y en muchos de la primera generación de Pentium.

Este tipo de chips que su nombre completo es FÁST PAGE MODE RAM porque permiten que parte de su almacenamiento puede ser leído sin introducir estados de espera. Ellos dividen su espacio total de direcciones en pequeñas secciones llamadas páginas, usualmente de 2Kb es decir incorpora un sistema de paginado debido a que se considera probable que el próximo dato a acceder esté en la misma fila, ganando tiempo en caso afirmativo. Es decir se deja activada la fila ganándose ese tiempo cuando se accede a otro dato. Normalmente, las transferencias de datos desde las memorias se realizan en paquetes de 4 datos llamados Burst. Por esta razón el rendimiento de un tipo de memoria se expresa por 4 números separados por guiones que son los ciclos de reloj que la memoria necesita para responder. Así la memoria ideal sería 1-1-1-1 que significa que en cada ciclo de reloj se transfiere un dato.

La velocidad de respuesta de la memoria se mide en nanosegundos (ns). Para un bus de 66Mhz con el esquema antes citado se requieren memorias de 60ns. Con buses de menor velocidad (por ejemplo Pentium 120 y 150) es suficiente con memorias de 70ns.

Viendo el sistema desde otro punto de vista tenemos que con memoria FPM de 60ns se alcanzan anchos de banda de 28.5Mhz distante de los 66Mhz del bus y aun mucho más de la velocidad del micro. Por lo que podemos decir que desde el ya olvidado 80286 de Intel, las memorias no han podido competir con las frecuencias de los microprocesadores, por lo que el micro se detiene a esperar que la memoria le entregue el anhelado dato, que puede ser la siguiente instrucción a ejecutar como cualquier otra información.

EDO RAM

La memoria EDO incorpora una pequeña modificación técnica en la FPM, de tal forma que la que la operación FPM se convierte en dos estados pipeline (Por así decirlo, procesados a la vez). Con ello, los datos siguen estando disponibles en el bus de la memoria mientras la siguiente dirección es preparada. A esto se le llama EXTENDED DATA OUTPUT, de donde recibe el nombre de EDO RAM.

La EDO es la memoria más popular en nuestros tiempos por dos razones:

La velocidad de acceso se incrementa notablemente.

Los fabricantes han tenido que hacer muy pocos cambios respecto a la FPM.

Su principio de funcionamiento es muy similar al anterior, se activa la primera fila y luego es habilitada la columna. La diferencia ocurre, al reactivar el pulso de

activación de columnas para el siguiente acceso, una vez que el dato está disponible, y desconectar el buffer de datos. La memoria EDO mantiene validado el buffer de datos aun durante la caída del pulso de selección de columnas (CAS) para la precarga del próximo ciclo. De esta forma los tiempos de precarga de la señal CAS pueden solapar el tiempo de validación de datos, ganándose tiempo para el subsiguiente ciclo.

La EDO puede trabajar, en el caso más favorable, con un esquema 5-2-2-2, lo que supone una mejoría hasta del 40% en el rendimiento global. A pesar de todo, el ancho de banda alcanza con memorias de 60ns es de 40Mhz, todavía distante de los 66Mhz del bus de un PC.

Las memorias EDO tienen sus días contados. La razón es que se ha llegado a un límite impuesto por el diseño de FPM, parcialmente enmendado en las EDO. Hemos visto que la EDO más rápida no puede alcanzar la frecuencia de bus de 66Mhz y si sumamos el avance tecnológico que han logrado buses de 75 y 83.3Mhz vemos que las memorias tienen que cambiar su principio de funcionamiento, además Intel plantea lanzar al mercado un bus de 100Mhz, siendo más necesario lo antes dicho.

BEDO (Burst EDO)

La memoria BEDO es un avance sobre la EDO destinada específicamente al mercado de los PC. Es capaz de conseguir un esquema de 5-1-1-1 y con un tiempo de acceso de 50 ns. es capaz de alcanzar los 66 MHz. Es un tipo de memoria poco común y no ha sido muy utilizada debido al surgimiento de las SDRAM.

SDRAM o DRAM sincrónica

Las SDRAM son una nueva generación de tecnología de las DRAM que les permite usar el mismo reloj que el bus del procesador. Esta memoria va a solucionar tanto los problemas actuales como los que van a surgir con el nacimiento del Bus de 100Mhz. Esto lo ha conseguido con un diseño desde cero, rompiendo con la tendencia impuesta por la memoria FPM. Las memorias EDO y FPM son asincrónicas y no tienen señal de reloj.

DRAM sincrónica o SDRAM es la primera tecnología de memorias DRAM diseñadas para sincronizarse a sí misma con los tiempos del bus. A diferencia de las anteriores la SDRAM tiene una entrada de reloj al igual que el microprocesador y sus operaciones son igualmente controladas, es decir, que el controlador de memoria conoce el momento exacto en el que los datos están disponibles, sin necesidad de esperas innecesarias por parte del micro entre accesos a la memoria.

Por otra parte el núcleo DRAM es mucho más rápido que el de las memorias convencionales, llegando a alcanzar velocidades hasta 4 veces superiores. Una arquitectura de doble banco los cuales trabajan entrelazados, de forma que cuando un banco prepara los datos el otro los proporciona. Así mismo, la longitud del burst

Elementos de Arquitectura y Seguridad Informática

es programable permitiendo un diseño flexible en función del sistema que deba soportarlo.

El esquema de trabajo de la SDRAM es de 5-1-1-1. Con memorias de 15ns podemos alcanzar el celebre 66Mhz y con memorias de 10ns llegaremos a 100Mhz, muy recomendables cuando pasamos la barrera de los 66Mhz en el bus. Podemos decir que esta memoria se eleva como única alternativa para solucionar los problemas de velocidad que existen hasta hoy en día. Por otro lado, parte del futuro del AGP (Puerto acelerador de gráficos) que permite que las tarjetas gráficas utilicen la memoria principal del sistema es posible gracias a las memorias SDRAM.

La SDRAM se presenta en forma de **DIMM** de 128 pines y 64 bits de datos y opera a 3.3V. Algunos de los DIMM's más viejos están fabricados con memorias FPM o EDO y operan solamente a 5V, note que estos no deben ser confundidos con los SDRAM DIMM.

Selección de parámetros de la SDRAM en el BIOS

Existe un parámetro importante que afecta las prestaciones de las SDRAM, el CAS Latency Time. Este es similar al CAS Access Time de las EDO DRAM y se calcula en números de estados de reloj (clock state). El Chipset INTEL TX soporta 2 o 3 relojes para el CAS Latency Time. Sin embargo, existen SDRAM que no aceptan estos requerimientos de los Chipset INTEL TX. Si la memoria SDRAM tiene problemas de inestabilidad revise en el BIOS setup Chipset Features la opción SDRAM(CAS Lat/RAS-to-CAS), cámbielo de 2/2 a 3/3, lo cual significa 3 clocks CAS Latency.

Tipos de memorias y latencia

La siguiente tabla muestra algunas memorias y los tiempos de latencia.

Tabla II-11

FABRICANTE	MODELO	CAS LATENCY TIME
Samsung	KM416511220AT-G12	2
NEC	D4S16162G5-A12-7JF	2
Hitachi	HM5216805TT10	2
Fujitsu	81117822A-100FN	2
TI	TMX626812DGE-12	2
TI	TMS626812DGE-15	3
TI	TMS626162DGE-15	3
TI	TMS626162DGE-M67	3

Tabla II-12

	BIT 1	BIT 2	BIT 3	BIT 4	Ciclos de espera/ Burst
FPM DRAM	5	3	3	3	10
EDO DRAM	5	2	2	2	7
BEDO DRAM	5	1	1	1	4 (No se comercializa)
SDRAM	5	1	1	1	4
L2(SDRAM)	2	1	1	1	1

Tabla II-13

	FPM	EDO	BEDO	SDRAM
Especificación (cod.)	-5,-6,-7	-5,-6,-7	-5,-6,-7	-10,-12,-15
Especificación (ns)	50,60,70	50,60,70	50,60,70	10,12,15
Velocidad de la memoria (Mhz)	33,28,25	50,40,33	66,60,50	100,80,66

DDR SDRAM

Para el futuro las memorias DDR SDRAM (Double Data Rate SDRAM) constituirán una versión mejorada de las SDRAM. Esta memoria es sincrónica al igual que la anterior pero transfiere información tanto en el flanco de subida como en el de bajada del pulso de reloj, con lo cual duplica la cantidad de información a transmitir. Según esto hablamos de un ancho de banda de 200Mhz. Pero por el momento esta tecnología necesitara esperar algún tiempo hasta que el mercado precisé de valores tan extremos (con relación a nuestro tiempo).

¿Cuál es el futuro en la memoria RAM?.

Actualmente se prevén tres posibles sucesores de la SDRAM, estos son:

RDDRAM

Desarrollado por Intel y Rambus. Este último no es actualmente un fabricante de memorias, sino que diseña una interface de memoria de alta velocidad y lo licencia a nueve fabricantes líderes de memorias.

Rambus puede manejar su bus especial de 16 Bits a velocidades de hasta 600 MHz y añade cerca de 100 MHz por año. Por el momento RDRAM puede alcanzar un ancho de banda sobre un Bus de 16bits de 1.6 Gb/s, el doble de rapidez de las DRAM a 100 MHz. Sobre un Bus de 32 bits el ancho de banda se duplica nuevamente a 3,2 Gb/s. Rambus plantea que su Bus de memoria podría eventualmente correr a 1000 MHz (1 GHz), alcanzando un ancho de banda de 4 Gb/s.

SLDRAM

Es un standard propuesto por 22 compañías, incluyendo Apple, Hewlett-Packard, IBM, Motorola, NEC, y Texas Instruments.

Aunque el standard no está finalizado, SLDRAM será capaz también de rangos de transferencias del orden de los Gigabytes.

DDR SDRAM o SDRAM II (Double Data Rate SDRAM).

Este tipo de DRAM que es sincrónica al igual que la SDRAM, añade la capacidad de doble reloj, es decir transfiere la información tanto en el flanco de subida como en el de bajada de cada ciclo de reloj, con lo cual duplica la cantidad de información que puede transferir. Según esto, hablaríamos de un ancho de banda de justo el doble, es decir, 200MHz, con lo cual tendríamos en el bus del PC tasas de hasta 1.6 Gb/s.

SIMMs y DIMMs

Algo que no tiene nada que ver con el tipo de memoria y sí con su empaquetado es lo de los módulos SIMM y DIMM. En efecto antiguamente las memorias se incorporaban al ordenador en integrados sueltos que se pinchaban en zócalos. Ahora vienen en módulos que encajan en unos raíles. Los módulos más comunes son los SIMM(Single in Line Memory Module) de 72 contactos y 32 bits y los DIMM(Dual in Line Memory Module) de 168 contactos y equivalentes a dos módulos SIMM.

Queremos enfatizar que el empaquetado no tiene nada que ver con las prestaciones ni con la calidad de la memoria y que hay que tener en cuenta la disponibilidad en uno u otro formato de los diferentes tipos de memoria.

Se trata de la forma en que se juntan los chips de memoria, del tipo que sean, para conectarse a la placa base del ordenador. Son unas plaquitas alargadas con conectores en un extremo; al conjunto se le llama módulo. El número de conectores depende del bus de datos del microprocesador, que más que un autobús es la carretera por la que van los datos; el número de carriles de dicha carretera representaría el número de bits de información que puede manejar cada vez.

SIMMs: Single In-line Memory Module, con 30 ó 72 contactos. Los de 30 contactos pueden manejar 8 bits cada vez, por lo que en un 386 ó 486, que tiene un bus de datos de 32 bits, necesitamos usarlos de 4 en 4 módulos iguales. Miden unos 8,5 cm (30 c.) ó 10,5 cm (72 c.) y sus zócalos suelen ser de color blanco. Los SIMMs de 72 contactos, más modernos, manejan 32 bits, por lo que se usan de 1 en 1 en los 486; en los Pentium se haría de 2 en 2 módulos (iguales), porque el bus de datos de los Pentium es el doble de grande (64 bits).

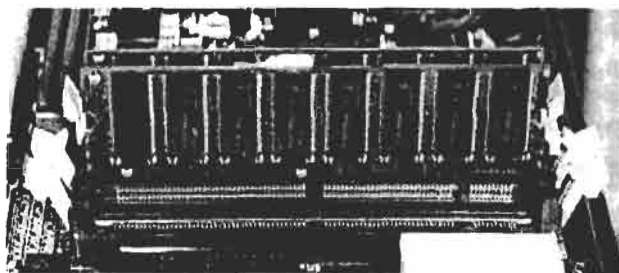


Figura II.9. Vista de la forma de colocar las memorias DIMM

DIMMs: más alargados (unos 13 cm), con 168 contactos y en zócalos generalmente negros; llevan dos muescas para facilitar su correcta colocación (Figura II.9). Pueden manejar 64 bits de una vez, por lo que pueden usarse de 1 en 1 en los Pentium o Pentium II. Existen para voltaje estándar (5 voltios) o reducido (3.3 V).

RIMM: módulo de memoria RDRAM (Rambus).

La **RDRAM o memoria Rambus** se planteó como una solución a esta necesidad, mediante un diseño totalmente nuevo. La Rambus tiene un **bus de datos más estrecho, de sólo 16 bits = 2 bytes, pero funciona a velocidades mucho mayores**, de 300, 356 y 400 MHz. Además, **es capaz de aprovechar cada señal doblemente**, de forma que en cada ciclo de reloj envía 4 bytes en lugar de 2.

Debido a este doble aprovechamiento de la señal, se dice que la Rambus funciona a 600, 712 y 800 MHz "virtuales" o "equivalentes". Y por motivos comerciales, se la denomina PC600, PC700 y PC800. Por todo ello, su capacidad de transferencia es:

Rambus PC600: $2 \times 2 \text{ bytes/ciclo} \times 300 \text{ MHz} = 1,2 \text{ GB/s}$

Rambus PC700: $2 \times 2 \text{ bytes/ciclo} \times 356 \text{ MHz} = 1,42 \text{ GB/s}$

Rambus PC800: $2 \times 2 \text{ bytes/ciclo} \times 400 \text{ MHz} = 1,6 \text{ GB/s}$

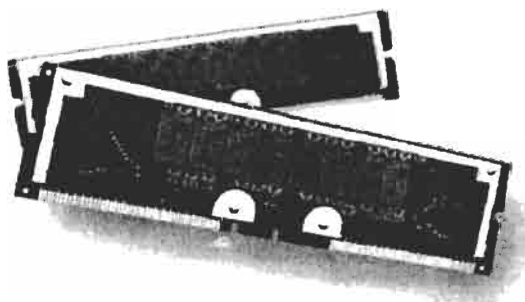


Figura II.10. Vista de la memoria Rambus o PC 133.

Elementos de Arquitectura y Seguridad Informática

Como vemos, la Rambus más potente (la de "800 MHz equivalentes") puede transmitir el doble de datos que la SDRAM PC100, lo que no es poco... pero no es ocho veces más, como a muchos publicistas les gusta hacer creer.

¿Qué es mejor: Rambus o PC133?

Si la pregunta fuera: ¿es la Rambus más rápida que la PC133?, responderíamos que sí, sin lugar a dudas. Pero ¿merece la pena esa diferencia de velocidad? Esto ya es más complicado de evaluar...

Aunque teóricamente la Rambus puede alcanzar 1,6 GB/s y la PC133 (Figura II.10) "sólo" 1,06 GB/s, esto **NO** quiere decir que un PC con memoria Rambus vaya a ser un 50% más rápido que otro con PC133; en absoluto. Para apreciar las diferencias, deberemos encontrarnos en un caso en que el microprocesador quiera (y pueda) aprovechar ese ancho de banda extra durante un tiempo apreciable, lo cual no es tan sencillo.

Por ejemplo, puede que el cálculo se realice con unos pocos datos que estén en las rápidas memorias caché, en cuyo caso no se accederá a la memoria principal; o que se deba acceder a un dispositivo mucho más lento como el disco duro, lo que echa a perder cualquier ganancia que hayamos obtenido; o que el cuello de botella se encuentre en una tarjeta gráfica incapaz de procesar los datos que le mandamos; o que el micro no calcule lo suficientemente rápido como para aprovechar la diferencia; o sencillamente que el ahorro de tiempo sea inapreciable (no sé a usted, pero a mí me cuesta un poco distinguir entre 0,03 segundos y 0,04 segundos).

Para aprovechar la ventaja que ofrece la Rambus, deberemos utilizar **aplicaciones de carácter altamente profesional**: cálculo de renderizados tridimensionales y servidores sobrecargados de trabajo y usuarios, por ejemplo.

En esta clase de programas, la utilización de la Rambus puede aumentar el rendimiento entre un 5% y un 15%, según concienzudos análisis publicados en uno de los mejores sitios web sobre hardware, www.anandtech.com; en cambio, **en aplicaciones más normales como ofimática o juegos la diferencia entre PC133 y Rambus es casi insignificante**, en el mejor de los casos entre un 1% y un 5% (y a veces, un 0% redondo).

Pero independientemente de si es mejor o no, la Rambus se enfrenta a varios problemas serios que no tiene la PC133, como veremos a continuación. Uno de ellos es, los numerosos problemas de compatibilidad entre ellos y con las diferentes placas base...

Porque éste es otro de los problemas a los que se enfrenta la Rambus: es **una tecnología excesivamente reciente**.

Un ejemplo: aunque casi nadie lo comenta, "no todas las Rambus son iguales"; como vimos, existen 3 velocidades distintas a las que puede funcionar: 300, 356 y 400 MHz (PC600, PC700 y PC800). Recordemos que para alcanzar el sí muy comentado valor de 1,6 GB/s de transferencia, se necesitan módulos del último tipo.

Evidentemente, esos módulos de 800 MHz (MHz "equivalentes", como explicamos más arriba) son los de mayor calidad y los más caros. Son tan difíciles de fabricar que pocas empresas lo han realizado con éxito. Además, la capacidad máxima de memoria del sistema se verá limitada por el escaso número de ranuras disponibles en la placa base, algo paradójico si pensamos que en los ambientes profesionales, donde esta memoria podría ser aprovechada 128 MB se considera una cifra casi ridícula, no siendo extraño encontrar equipos con 512 MB... o más.

Unidad Central De Procesamiento (CPU)

Caché

El procesador pide información más rápidamente de lo que la memoria principal del sistema es capaz de brindarle, por esta razón este introduce estados de espera (Wait State), esencialmente el procesador no hace nada hasta que no recibe la información solicitada. Esto afecta grandemente las prestaciones del sistema. Cuando este corre sin necesidad de estados de espera se dice que el sistema esta en operación de cero estados de espera (**0 WS**) y corre mucho más rápido.

La velocidad de la memoria, como hemos mencionado, se mide en nanosegundos (ns). Los chips de memoria DRAM más veloces, disponibles en estos momentos, son de 70 o 60 ns. Para que un procesador opere en el modo de **0 WS** sobre una tarjeta madre con frecuencia de reloj de 33 MHz. (Procesadores 486DX/33, 486DX2/66, 486 DX4/100) el sistema de memoria debe responder a una velocidad de 30 ns; mientras que sobre tarjetas madres a 66Mhz (Procesadores Pentium 100/133/166) la memoria debería operar a 15 ns. Lo cual es equivalente a que el sistema debería trabajar con memoria SRAM que como ya sabemos es más rápida que la DRAM (por que no requiere refrescamiento) pero cuesta cerca de 10 veces más, por esta razón es que no son usadas como almacenamiento primario de las PC's.

Aquí es donde entra a trabajar la Memoria Cache, que no es más que un bloque de memoria muy rápida (típicamente RAM estática de muy alta velocidad, con tiempos de acceso de 15 a 35 ns) interpuesta entre el microprocesador y la memoria principal del sistema.

El objetivo de esta memoria es lograr que el microprocesador trabaje con la memoria a su velocidad de procesamiento. Lo cual permite que el sistema en general aumente sus prestaciones ya que no tiene que introducir estados de espera.

Para empezar, digamos que la caché no es sino un tipo de memoria del ordenador; por tanto, en ella se guardarán datos que el ordenador necesita para trabajar. ¿Pero no era eso la RAM?, preguntará usted. Bueno, en parte sí. A decir verdad, la memoria principal del ordenador (la RAM, los famosos 8, 16, 32 ó 64 "megs") y la memoria caché son básicamente iguales en muchos aspectos; la diferencia está en el uso que se le da a la caché.

Elementos de Arquitectura y Seguridad Informática

Debido a la gran velocidad alcanzada por los microprocesadores desde el 386, la RAM del ordenador no es lo suficientemente rápida para almacenar y transmitir los datos que el microprocesador (el "micro" en adelante) necesita, por lo que tendría que esperar a que la memoria estuviera disponible y el trabajo se ralentizaría. Para evitarlo, se usa una memoria muy rápida, estratégicamente situada entre el micro y la RAM: la memoria caché.

Ésta es la baza principal de la memoria caché: es muy rápida. ¿Cuánto es "muy rápida"? Bien, unas 5 o 6 veces más que la RAM. Esto la encarece bastante, claro está, y ése es uno de los motivos de que su capacidad sea mucho menor que el de la RAM: un máximo en torno a 512 kilobytes (512 Kb), es decir, medio "mega", frente a 16 ó 32 megas de RAM. Además, este precio elevado la hace candidata a falsificaciones y timos.

Pero la caché no sólo es rápida; además, se usa con una finalidad específica. Cuando un ordenador trabaja, el micro opera en ocasiones con un número reducido de datos, pero que tiene que traer y llevar a la memoria en cada operación. Si situamos en medio del camino de los datos una memoria intermedia que almacene los datos más usados, los que casi seguro necesitará el micro en la próxima operación que realice, se ahorrará mucho tiempo del tránsito y acceso a la lenta memoria RAM; esta es la segunda utilidad de la caché.

La caché interna

Nivel 1 y Nivel 2

La caché a la que nos hemos referido hasta ahora es la llamada "caché externa" o de segundo nivel (L2). Existe otra, cuyo principio básico es el mismo, pero que está incluida en el interior del micro; de ahí lo de interna, o de primer nivel (L1).

Esta caché funciona como la externa, sólo que está más cerca del micro, es más rápida y más cara, además de complicar el diseño del micro, por lo que su tamaño se mide en pocas decenas de kilobytes. Se incorporó por primera vez en los micros 486, y por aquel entonces era de 8 Kb (aunque algunos 486 de Cyrix tenían sólo 1 Kb). Hoy en día se utilizan 32 ó 64 Kb, aunque seguro que pronto alguien superará esta cifra.

La importancia de esta caché es fundamental; por ejemplo, los Pentium MMX son más rápidos que los Pentium normales en aplicaciones no optimizadas para MMX, gracias a tener el doble de caché interna. A decir verdad, la eficacia de la "optimización MMX" de aplicaciones como Microsoft Office, está por ver...

Todos los procesadores Intel desde el surgimiento del 486 incorporan en su interior una pequeña cantidad de este tipo de memoria (entre 8 y 16 Kb). Cuando la memoria cache está integrada al procesador se le conoce como Cache Interna o de Primer Nivel (L1). En la tabla siguiente se muestran algunas de las capacidades típicas de cache de primer nivel en los procesadores Intel.

Tabla II-14

Microprocesador	Capacidad	Observaciones
i486 SX/SL/DX/DX2	8 Kb	Cache de datos y códigos común.
i486 DX4	16 Kb	Cache de datos y códigos común.
Pentium	16 Kb	Cache de datos (8Kb) y código (8Kb) común.
Pentium MMX	32 Kb	Cache de datos (8Kb) y código (8Kb) común.
Pentium Pro		Incorpora la L2 cache (256/512 KB) dentro del procesador y la arquitectura DIB.

Existe también una Cache Externa o Cache de segundo nivel (Level two, L2) que está sobre la tarjeta madre y es administrada por un controlador de memoria Cache. Capacidades típicas de esta memoria pueden ser: 128KB, 256KB ó 512KB y en un futuro alcanzar los 1024 KB. En los sistemas Pentium actuales es 512 Kb la cantidad de memoria cache externa más común.

Normalmente la memoria Cache, tanto la Interna como la Externa, pueden habilitarse o no. Esto normalmente se configura en el **SETUP** del **BIOS**. Por ejemplo en el **BIOS AWARD** en la sección **BIOS FEATURES SETUP** aparecen las siguientes opciones:

CPU internal Cache: Enable/Disable
 External Cache: Enable/Disable

También hay opciones en el **BIOS CHIPSET SETUP** que permiten que las direcciones correspondientes al BIOS del sistema (F000-FFFF H) y al BIOS de Video (C000-C7FF H) se pasen por la memoria Cache, logrando así un aumento adicional de la velocidad de acceso a estas áreas de memoria.

System BIOS Cacheable Enable/Disable

El costo es la mayor desventaja que tiene utilizar gran cantidad de memoria Cache. Esta puede influir grandemente en el costo promedio del sistema. Por esta razón la mayoría de las tarjetas madres 486 y las primeras que soportaban procesadores Pentium permiten escalar la memoria cache a la medida del usuario final.

Métodos de actualización de la memoria principal.

Es necesario que el contenido de la memoria principal y su bloque correspondiente en la memoria cache sean iguales en su contenido. Para lograr esto se han implementado dos métodos de actualización de la memoria principal

Write Through (escritura a través): en el que se escriben los datos en memoria RAM y en memoria cache simultáneamente.

Write Back (escritura atrasada): en el cual se actualizan solamente los datos en la memoria cache, y solo se escribe en la RAM cuando el bloque se va usar para mapear otro pedazo de la RAM. Este método permite aún más rapidez, puesto que solo se escribe en la RAM en el momento que es necesario.

En algunos procesadores i486 la cache interna y externa podía trabajar con cualquiera de estos métodos, Nuevamente era en el SETUP del BIOS donde se seleccionaba el método que se iba a emplear. Todos los procesadores Pentium y tarjetas madres que los soportan implementan el Método **Write Back**.

Organización lógica de la memoria cache.

La organización lógica de una cache implica como se organiza la cache, como se direccionan y colocan los datos dentro de ella.

Para entender esta organización debemos aclarar primero que la unidad de transferencia entre memoria principal y memoria cache de denomina Línea o Bloque. Un Bloque está formado por un conjunto de palabras contiguas. Debe contemplarse a la memoria cache como un conjunto de bloques físicos capaces de contener bloques de la memoria principal.

La colocación del bloque en memoria cache y la cantidad de bloques que hay que examinar para ver si es fallo o acierto, dependen de la correspondencia que se ha escogido en su diseño. Un determinado bloque de memoria cache se corresponde con determinados bloques de memoria principal; de ahí que en caso de fallo y según la correspondencia escogida, solo sea necesario examinar una pequeña parte de la cache.

Existen tres tipos fundamentales de correspondencia:

Correspondencia directa: solo debe examinarse un bloque.

Correspondencia asociativa por conjuntos: se examinan un determinado número de bloques.

Correspondencia completamente asociativa: se examinan todos los bloques de la cache.

En la memoria cache por cada bloque residente se guardan, por tanto, dos informaciones:

- El contenido de las palabras consecutivas que constituyen el bloque.
- La marca (Tag) del bloque. Es un número variable de bits dependiendo de la correspondencia empleada.

Selección de la velocidad de la Memoria cache.

Utilice memorias SRAM de 20 ns para frecuencias en el bus de 50/60 Mhz (Pentium 75/90/100/120/150) y SRAM de 15 ns para frecuencias de 66 MHz (Pentium 100/133/166/200)

PBSRAM (Pipelined Burst SRAM).

Este es un tipo de memoria cache desarrollada para trabajar con los procesadores Pentium. En estos el modo de acceso a la memoria en Ráfaga (Burst) significa la lectura continua de cuatro QWord (una Quad-Word es equivalente a $4 \times 16 \text{ bits} = 64 \text{ Bits}$) y únicamente es necesario la decodificación por la SRAM de la primera dirección.

La PBSRAM automáticamente envía las restantes tres QWords hacia el CPU de acuerdo a una secuencia predefinida. El tiempo normal de decodificación de la dirección para la SRAM es de 2 a 3 relojes. Esto hace que el atiemppamiento de lectura de datos del CPU para cuatro Qwords sea al menos 3-2-2-2 con un total de 9 relojes si se usan memorias SRAM asincrónicas tradicionales.

Sin embargo, con PBSRAM no es necesario decodificar las direcciones para las restantes tres QWords. Por tanto el atiemppamiento de lectura de datos puede ser 3-1-1-1, lo cual es equivalente a 6 relojes y es mucho más rápido que las SRAM asincrónicas.

Las velocidades cada vez más rápidas de los CPU actuales requieren de tarjetas madres con un complejo diseño de atiemppamiento. Cada línea de circuito impreso y la demora de los componentes debe tomarse en consideración. El diseño del SLOT de expansión de la Cache causaría demoras de 2 a 3 ns en el atiemppamiento de la PBSRAM y la longitud del camino desde el modulo de cache a través de los contactos metálicos podría demorar este atiemppamiento 1 o 2 ns más. Esto podría resultar en un sistema inestable una vez que el módulo y el SLOT se calienten.

Esta es la razón por la que la mayoría de las tarjetas madres actuales que soportan este tipo de memoria cache la tienen ya soldadas y generalmente no es posible hacer ninguna actualización de memoria cache. Es importante tener en cuenta que 512 KB de PBSRAM brindan cerca de 3% más de prestaciones que 256KB y la diferencia de precio es mínima, por esta razón es conveniente comprar tarjetas madres que soporten 512KB en vez de 256KB.

Elementos de Arquitectura y Seguridad Informática

Hace algún tiempo, las cache aportaban un gran rendimiento al sistema dado que los principios que seguían eran los adecuados: accesos probables dentro de un mismo rango de memoria, aplicaciones de tamaño moderado, etc.

Hoy en día, ha surgido el gran enemigo del cache: la multitarea. Es decir, múltiples procesos ejecutándose simultáneamente, cada uno (de los cuales tiene su porción de código, y datos en áreas no adyacentes. La solución sólo puede tener dos vertientes: un tamaño de cache mayor (mínimo 512 K) y mucho mejor, una memoria principal más rápida

El tamaño de la caché

Leído lo anterior, usted pensará: pues cuanto más grande, mejor. Cierto, pero no; o más bien, casi siempre sí. Aunque la caché sea de mayor velocidad que la RAM, si usamos una caché muy grande, el micro tardará un tiempo apreciable en encontrar el dato que necesita. Esto no sería muy importante si el dato estuviera allí, pero ¿y si no está? Entonces habrá perdido el tiempo, y tendrá que sumar ese tiempo perdido a lo que tarde en encontrarlo en la RAM.

Por tanto, la caché actúa como un resumen, una "chuleta" de los datos de la RAM, y todos sabemos que un resumen de 500 páginas no resulta nada útil. Se puede afirmar que, para usos normales, a partir de 1 MB (1024 Kb) la caché resulta ineficaz, e incluso pudiera llegar a ralentizar el funcionamiento del ordenador. El tamaño idóneo depende del de la RAM, y viene recogido en la siguiente tabla:

Se debe hacer notar que muchos "chipsets" para Pentium, como los conocidos Intel "Tritón" VX o TX, no permiten cachear más de 64 MB de RAM; es decir, que a partir de esta cifra, **ES COMO SI NO EXISTIERA CACHÉ EN ABSOLUTO (0 Kb!!)**.

Así que si necesita instalar más de 64 MB en una placa para Pentium, busque una placa que permita cachear más de esa cifra (como algunas -no todas- las que tienen chipsets "Tritón" HX.

La caché de los Pentium II y Mendocino

Puede que haya oído hablar de que los Pentium II (y su antecesor el extinto Pentium Pro) tienen 512 Kb de caché interna; esto es inexacto, cuando no una "confusión interesada" por parte de Intel y los vendedores. Los Pentium II tienen 64 Kb de caché interna, y 512 Kb de caché dentro del cartucho SEC pero externa al encapsulado del microchip.

Este contrasentido se explica si se ve un Pentium II "destripado" como éste:

Dentro de la gran carcasa negra encontramos una placa de circuito en la que va soldado el micro en sí (en el centro de la imagen), junto con varios chips que forman la caché, externa a lo que es propiamente el micro. Sin embargo, esta caché funciona a una frecuencia que es la mitad de la del micro (es decir, a 116, 133 MHz o más), y no a la de la placa base como la caché externa clásica (de 50 a 66 MHz en los Pentium o 100 MHz en los AMD K6-2).

Los que casi pueden presumir de tener una gran caché interna son los Celeron Mendocino (no los Celeron normales, que carecen de caché L2 en absoluto). Estos micros tienen sus 128 Kb de caché L2 integrada en el propio encapsulado del micro y la hacen funcionar a la misma velocidad que éste, de forma que no llega a ser tan rápida como la caché L1 pero sí lo bastante como para permitirles competir con los Pentium II pese a tener sólo la cuarta parte de caché.

Digamos, en fin, que los Pentium II y los Celeron Mendocino tienen una caché interna y una semi-externa, lo cual no es poco mérito en absoluto; pero las cosas son como son, mal que le pese a los magos de la publicidad.

Sobre cachés falsas y tramposos

Como ya dijimos, la caché es un bien preciado. Por ello, la natural codicia de ciertos personajes les ha llevado a fabricar placas base con chips de caché de vulgar plástico sólido, método que puede enriquecer la placa y reducir el rendimiento del ordenador de un 5 a un 10%.

Este fenómeno tuvo su auge con las placas base para 486, aunque no se puede asegurar que esté totalmente erradicado. Desgraciadamente, hay pocos métodos para saber si un chip de caché es bueno o falso, y casi ninguno se basa en la observación directa (como no sea por radiografía). Los medios principales para detectar el fraude son:

observar chips sumamente burdos y mal rematados, con bordes de plástico y serigrafiados de baja calidad (suponiendo que sepa identificar el o los chips de caché, lo cual puede ser difícil);

utilizar alguna herramienta de diagnóstico por software que detecte la presencia o ausencia de caché.

Sobre estos programas de diagnóstico, cabe comentar que no son infalibles, por lo que si alguno no detecta la caché conviene probar con otro (pero conque uno la detecte, es casi seguro que es auténtica). Además, pueden fallar con ciertos tipos muy rápidos y modernos de caché, por lo que no suele servir el mismo programa para la placa de un 486 y la de un Pentium. Algunos de estos programas (para placas 486, que suelen ser las más falsificadas) se pueden encontrar en Internet.

Si usted acaba convencido de que su placa tiene una caché falsa (aunque si se trata de una para Pentium puede llevarle su tiempo), lo mejor que puede hacer es no volver a comprar en la tienda donde la adquirió o, si tiene tiempo y ganas, irse a quejar. No es probable que le hagan caso, pero ¡que le oigan! (Y si les engañó su proveedor, no es excusa, sino falta de profesionalidad.)

Tecnologías usadas en la caché

Aunque en general no se puede elegir qué memoria caché adquirir con el ordenador, puesto que se vende conjuntamente con la placa base (o con el micro, si

Elementos de Arquitectura y Seguridad Informática

es un Pentium II o un Mendocino), conviene tener claros unos cuantos conceptos por si se diera el caso de tener varias opciones a nuestra disposición.

Ante todo, el tipo de memoria empleada para fabricar la caché es uno de los factores más importantes. Suele ser memoria de un tipo muy rápido (como por ejemplo SRAM o SDRAM) y con características especiales, como burst pipeline: transmitir datos "a ráfagas" (burst).

La velocidad de la caché influye en su rendimiento, como es obvio. Las cachés se mueven en torno a los 10 nanosegundos (ns) de velocidad de refresco; es decir, que cada 10 ns pueden admitir una nueva serie de datos. Por tanto, a menor tiempo de refresco, mayor velocidad.

El último parámetro que influye en las cachés es la forma de escribir los datos en ellas. Esto se suele seleccionar en la BIOS, bien a mano o dejando que lo haga el ordenador automáticamente; las dos formas principales son:

Write-Through: impronunciable término que indica el modo clásico de trabajo de la caché;

Write-Back: un modo más moderno y eficaz de gestionar la caché.

Cuál es el futuro de las memorias Cache?.

Los retos que esperan a los diseñadores de tarjetas madres con los niveles de frecuencia en memoria cache, son enormes. Aún cuando el CPU y la cache están aislados en módulos optimizados de Multiprocesamiento Simétrico (**SMP**, Symmetric Multiprocessing) como es el caso de las tarjetas madres que soportan la familia de los Pentium II y multiprocesadores 21264 Alpha. Esto hace necesario mover el control de la cache completamente al CPU través de un bus dedicado a la cache, el cual está físicamente separado del bus de memoria principal. A pesar de esto un nuevo tipo de SRAM podría aparecer en las memorias cache de las PC, esta es:

Late-Write Burst SRAM: (LWBRAM).

Permite aumentar la frecuencia hasta 200 MHz, suministrando el dato a escribir en la memoria un reloj después de la dirección. Estas SRAM ya están soportadas por algunos CPU RICS como Mips R10000/R12000, UltraSparc PA-8x00 y Alpha 21264.

III. MICROPROCESADORES AMD Y CYRIX 6X86

AMD

Este fabricante tejano que tantos dolores de cabeza dió a Intel con sus procesadores 386 y 486 tardó mucho en reaccionar ante el lanzamiento de la gama Pentium de INTEL. Lo hizo con el K5, pero la ventaja de INTEL era muy grande, pero con la compra de NEXGEN, se produjo un rápido avance que finalmente dio lugar al nacimiento del procesador K6.

En la actualidad AMD es un serio competidor de la gama Pentium MMX de Intel e incluso la gama Pentium II, y el anuncio de nuevos procesadores de este fabricante hace peligrar de nuevo la hegemonía del fabricante californiano como ocurrió en las gamas 386 y 486.

K5

Fue el primer procesador de la gama Pentium de 64 bits hecho por AMD de modo totalmente independiente, y de ahí su retraso en aparecer en el mercado.

AMD adoptó en estos procesadores el marcado de velocidad por comparación con el equivalente de INTEL, y no por la velocidad real interna de proceso, y se lanzaron versiones K5 PR-75 a K5 PR-166 con los mismos estadios intermedios de velocidad que los procesadores de INTEL.

Las prestaciones de este procesador son inferiores a las de los procesadores Pentium Clásicos (sin MMX), aunque mejores que las de los CYRIX 6x86 en operaciones de coma flotante (coprocesador matemático). Este procesador está superado por el K6 tanto en características y prestaciones.

K6

Cuando AMD compró NEXGEN, aprovechó el diseño de su procesador de la serie 686 de 64 bits para desarrollar el K6, un procesador destinado a competir con y superar al Pentium MMX, pero que ha resultado un serio competidor incluso para el Pentium II.

Al igual que el Pentium Clásico y el MMX, se instala en placas base con zócalo del tipo 7 (el de las placas Pentium) y se presenta en velocidades de 166MHz, 200MHz y 233MHz. Acaban de salir al mercado, con fecha 15 de Abril, las versiones de 266MHz y 300MHz, con tecnología de 0,25 micras, y aunque oficialmente no soportan la velocidad de bus de 100MHz, las pruebas hechas a 75MHz, 83MHz y 100MHz han dado unos resultados muy buenos y una estabilidad bastante alta, llegando a alcanzar los 400MHz. En cuanto a rendimiento comparado, el K-6

Elementos de Arquitectura y Seguridad Informática

300MHz compite seriamente con el Pentium II 300MHz excepto en operaciones de coma flotante.

Las características más importantes de este procesador son las siguientes:

- Integra las mismas instrucciones MMX que el Pentium MMX y el Pentium II de INTEL.
- Caché de nivel 1 de 64 KB (32KB para datos + 32KB para instrucciones), el doble que los Pentium MMX y Pentium II.
- Microarquitectura superescalar RISC86 (ejecución especulativa, ejecución fuera de orden, predicción avanzada de dos niveles, siete unidades de ejecución paralela).

Este procesador está más cerca del Pentium Pro y el Pentium II que del Pentium MMX en cuanto a desarrollo tecnológico, y de hecho esto queda refrendado por sus prestaciones, siempre superiores a las de un Pentium MMX a igualdad de velocidad, y muy cerca del Pentium II de igual velocidad, perdiendo respecto a éste solamente en operaciones que exigen una unidad de coma flotante rápida (coprocesador matemático).

Al igual que el Pentium MMX, exige placas que soporten voltaje dual (2,9/3,3 para las versiones K6-166 y K6-200, 3,2/3,3 para la versión K6-233) y 2,2/3,3 para las versiones K6-266 y K6-300, pero a diferencia de los Pentium MMX, no existen versiones OVERDRIVE, lo cual nos puede obligar a comprar una nueva placa base. Además, las versiones de 266MHz y 300MHz no son soportadas por muchas placas base, lo que nos puede obligar a un cambio de placa, pero la constante bajada de precio del Pentium II hace que tengamos nuestras dudas sobre el interés de su compra.

Esta es una muy buena compra, con una velocidad a camino entre Pentium MMX y Pentium II y con un precio incluso menor que el del Pentium MMX. Además las pruebas realizadas con un K6 300MHz haciendo OVERCLOCKING con el bus de 100MHz, no soportado oficialmente por el procesador, ha dado unos resultados que superan al Pentium II 300MHz (bus de 66MHz) excepto en operaciones de cálculo intensivo con la unidad de coma flotante.

Seguramente, ésta es la opción más recomendable para actualizar un equipo Pentium con placa que soporte voltaje dual aprovechando el resto de los componentes, siempre que sea posible. Si hay que comprar una nueva placa, hay que pensarlo seriamente, y escoger una de las nuevas placas con los últimos chipsets de VIA y ALI que soportan bus de 100MHz y AGP, de cara a poder utilizar los procesadores K6-2 de AMD y MII de CYRIX.

K6-2

AMD ha presentado el K6-2, antes llamado K6 3D, con bus de 100 MHz, 21 nuevas

instrucciones MMX, llamadas 3D NOW destinadas a mejorar el rendimiento en operaciones de coma flotante (CAD, juegos, multimedia, etc.) y velocidades iniciales de 266MHz, 300MHz y 333MHz, esperándose para el mes de Octubre la versión a 350MHz y antes de final de año las versiones de 400MHz y 500MHz, con lo que INTEL cada vez tiene más difícil mantener su cuota de mercado.

Las características más importantes de este procesador son las siguientes:

- Soporte oficial para el bus de 100 MHz en los modelos de 300MHz y 350MHz, y las futuras versiones de 400MHz y 450MHz. El modelo a 266MHz funciona con un bus de 66MHz, aunque funciona de manera estable, e incluso con mejores prestaciones, configurado como $100 \times 2,5 = 250$ MHz. La versión de 333MHz utiliza un bus de 95MHz, pero sus prestaciones son muy poco superiores al modelo anterior, debido a que el descenso del bus absorbe parcialmente el aumento de velocidad.
- A las 57 instrucciones MMX licenciadas por INTEL, añade 21 instrucciones a las que llama 3DNow!. Estas nuevas instrucciones están destinadas a mejorar los juegos 3D, el software con imágenes 3D, los programas de CAD, el audio 3D, el software de reconocimiento del habla, el funcionamiento de los WINMODEMS o modems HSP, etc.
- Caché de nivel 1 de 64 KB (32KB para datos + 32KB para instrucciones), el doble que los Pentium MMX y Pentium II.
- Caché de nivel 2 en placa base funcionando a la velocidad de bus.
- Ejecución de hasta 3 instrucciones 3D por cada ciclo de reloj.
- Ejecución de hasta 4 cálculos de coma flotante por cada ciclo de reloj.

Este procesador está destinado a competir directamente con el Pentium II, y comparando los nuevos procesadores de AMD con los Pentium II a igual velocidad (aunque con bus de 66MHz estos últimos), los resultados son asombrosos: en aplicaciones ofimáticas (procesador de texto, hoja de cálculo, etc.), el K6-2 llega a superar al Pentium II a igual velocidad, pero la ejecución de operaciones de coma flotante (CAD, multimedia, juegos, etc.) todavía es el dominio de INTEL. MICROSOFT ha anunciado que soportará las nuevas instrucciones de este procesador en su versión DirectX6 que podemos encontrar ya en la WEB de MICROSOFT.

Aunque este procesador tiene como complemento ideal las nuevas placas Super 7 (ver la sección de chipsets) con bus de 100MHz y AGP, diversas pruebas han demostrado que el K6-2 puede funcionar de forma estable sobre una placa con bus de 66MHz, configurando el procesador como 66x4 y como 66x4,5, siempre que la placa base admita el voltaje interno (CORE VOLTAGE) de 2,1V o 2,2V (este último es el oficial). Antes de comprar una nueva placa, deberíamos visitar la WEB del fabricante de nuestra placa base actual para comprobar esta posibilidad y buscar una BIOS actualizada.

Elementos de Arquitectura y Seguridad Informática

Además, a diferencia de los procesadores Pentium II con bus de 100MHz, que requieren memoria SDRAM PC-100, las placas Super 7 admiten memoria EDO y memoria SDRAM normal con el bus de 100MHz (siempre que ésta sea de calidad), lo que reduce sensiblemente el coste de la actualización, reduciendo las prestaciones en sólo un 10%.

En Enero de 1999 AMD presenta una nueva serie de su procesador K6-2 con velocidades de 366MHz (con bus de 66MHz), 380MHz (con bus de 95MHz) y 400MHz (con bus de 100MHz). La versión de 400MHz se caracteriza además por utilizar una nueva instrucción interna (WRITE MERGE BUFFER) que permite una gestión optimizada de la caché de nivel 1, con lo que sus prestaciones se acercan cada día más a las del Pentium II a igual velocidad de reloj. Esta nueva serie de procesadores con esta nueva instrucción, conocidos como CXT CORE, también se presentará con una velocidad de 350MHz.

Existen también versiones del K6-2 para portátiles, con velocidades de 266MHz, 300MHz y 333MHz.

K6-3

Anunciado inicialmente para final de 1998, pero deliberadamente atrasado hasta el primer trimestre del 99 para aprovechar el tirón del K6-2, AMD ha anunciado las características del K6-3, antes llamado K6-3D+.

Velocidades iniciales de 350MHz, 400MHz y 450MHz, esperando llegar a los 600MHz a final de 1999.

- Tecnología de 0'25 micras, esperando reducirla a 0'18 para final de año.
- Bus de 100MHz.
- Instrucciones 3DNow!
- 256KB de caché de nivel 2 en el propio procesador funcionando a la misma velocidad del procesador (como en el Pentium II XEON).
- La antigua caché de nivel 2 de la placa base pasa a ser caché de nivel 3 y funciona a la velocidad del bus.
- Capacidad para ejecutar 4 instrucciones simultáneamente.
- Compatibilidad con la mayoría de las placas Super 7. Solo se requiere que la placa soporte voltajes entre 2'3V y 2'5v, además de la preceptiva actualización de la BIOS.

Las pruebas preliminares de este procesador han dado unos resultados sorprendentes: a igual velocidad de procesador, iguala al Pentium II en aplicaciones ofimáticas.

CYRIX / IBM

Se convirtió con su 6x86 en el primer serio competidor a la gama Pentium de INTEL, llegando a superarlo en prestaciones, pero la aparición de los Pentium MMX los relegó totalmente, debido a la unidad de coma flotante más lenta de su procesador y la falta de instrucciones MMX. Luego el relevo fue tomado por AMD con su K6, pero de nuevo CYRIX ha vuelto a la arena con su nuevo 6x86MX (llamado también M2), con las 57 instrucciones MMX.

6x86

Fue el primer competidor serio a la gama Pentium, y aunque tuvo diversos problemas de compatibilidad, éstos fueron resueltos en las sucesivas revisiones o podían corregirse mediante parches que se podían obtener de la WEB de CYRIX. El nombre de estos procesadores, al igual que todos los de CYRIX hasta el momento pertenecientes a la gama de 64 bits, no viene dada por su velocidad, sino por sus prestaciones comparadas a los procesadores de Intel. Se presentaron versiones 6x86 P-120+ a 6x86 P-200+, con los mismos estadios intermedios que los procesadores de INTEL, y sus características más destacadas eran las siguientes:

Arquitectura superescalar.

- Predicción múltiple.
- Ejecución y proceso de datos fuera de orden.
- Caché de nivel 1 unificada de 16KB.

Debido a sus problemas de compatibilidad, especialmente el problema de la caché WRITE BACK con WINDOWS NT (resuelto en los procesadores con la revisión 2.7 o posterior), y sus problemas de sobrecalentamiento (resueltos con la serie 6x86L), su popularidad inicial descendió, y la aparición de los Pentium MMX, prácticamente los borró del mercado.

Otro problema añadido surgió con el 6x86 P-200+. Debido a que su velocidad de bus era de 75MHz, existían pocas placas base en el mercado que soportasen oficialmente esta velocidad, pero las más populares, con los chipsets 430HX y 430VX de Intel, daban frecuentes errores y problemas, aunque INTEL siempre advirtió que ambos chipsets no habían sido pensados para funcionar a 75MHz. Además muchos periféricos y componentes, como tarjetas gráficas, módulos de memoria y tarjetas SCSI, no funcionaban correctamente a la mitad de velocidad de reloj (38MHz), velocidad a la que funciona el bus PCI cuando la velocidad de bus es de 75MHz.

De todos modos, evitar este procesador y si acaso escoger el siguiente.

6x86L

Elementos de Arquitectura y Seguridad Informática

Básicamente es el mismo procesador que el anterior, pero con menor consumo de energía, para evitar los problemas de calentamiento que sufría el anterior.

El problema de este procesador es que utiliza el voltaje dual del Pentium MMX (2,8V/3,3V), por lo que no podrá instalarse en placas de cierta antigüedad.

Es un procesador rápido, pero sólo resulta interesante si se busca un ordenador de muy bajo coste.

6x86MX

Al igual que el K6 de AMD, este procesador debe situarse realmente a medio camino entre el Pentium MMX y el Pentium II. Por un lado ejecuta los programas ofimáticos más rápido que un Pentium MMX e incluso que un Pentium II en algunos casos, pero su unidad de coma flotante y sus prestaciones en 3D son algo inferiores a las de un Pentium MMX.

Este procesadores se ofrece actualmente en las siguientes versiones, con un marcaje de velocidad en función de su comparación con los procesadores de INTEL, que son 6x86MX PR-166GP, 6x86MX PR-200GP, 6x86MX PR-233GP, 6x86MX PR-266GP con velocidad de bus de 75x3 o 83x2,5 y voltaje interno de 2,7V, presentado en Enero de 1998 y en el mes de Abril ha presentado el 6x86MX PR-300GP de características similares al anterior, y, curiosamente, al mismo precio que la versión PR-266. Sus características más destacadas son:

- Caché de nivel 1 de 64KB unificada para datos e instrucciones.
- Incorpora las 57 instrucciones MMX licenciadas por INTEL.

Estos tres procesadores tienen la particularidad de poder escoger la velocidad de bus entre 50MHz y 75MHz, aunque esta última es la que ofrece las mejores prestaciones. De todos modos, para sacarle el máximo provecho y trabajar con un equipo estable, se debe escoger con sumo cuidado la placa base.

También se han detectado errores de compatibilidad como en las series anteriores, pero de igual modo, desde la página WEB de CYRIX podemos obtener los parches para corregirlos.

Es un gran procesador, de una gran rapidez, ligeramente más caro que los Pentium MMX y los K6 pero es recomendable con reservas debido a la velocidad de bus de 75MHz del 6x86MX PR-233GP y el 6x86MX PR-266GP. El vendedor debe asegurarnos que funcionará con la placa instalada. Imprescindible visitar la página WEB de CYRIX para ver la lista de placas probadas y compatibles con este procesador.

MII

Este procesador, anteriormente conocido por el nombre clave de CAYENNE es la nueva generación del 6x86MX, y pretende igualar e incluso mejorar las prestaciones del Pentium II mejorando la unidad de coma flotante (coprocesador matemático), la debilidad de todos los procesadores de CYRIX. Además integra 15 nuevas instrucciones multimedia para mejorar las prestaciones en multimedia y 3D y funciona con bus de 100MHz.

La nueva unidad de coma flotante es capaz de ejecutar 4 operaciones de coma flotante en cada ciclo de reloj usando instrucciones multimedia duales e incorpora 64KB de caché de nivel 1. Se puede encontrar ya en el mercado en versiones PR-300 y posteriormente veremos los PR-333, PR-350 y PR-400 para Navidad de 1998.

Como todos los procesadores CYRIX, la velocidad se calcula en relación a las prestaciones en comparación con los procesadores INTEL, y así el PR-300 funciona realmente a 233MHz, configurado como 66x3,5, aunque admite su configuración como 75x3, 83x2,5 o 100x2, siendo esta última la que ofrece mejores prestaciones.

Este procesador está fabricado con tecnología de 0,35 micras y su voltaje interno (CORE VOLTAGE) es de 2,9V, por lo que, al igual que sus hermanos, genera bastante calor, lo que siempre da lugar a un más que arriesgado overclocking.

Las primeras pruebas con este procesador mejoran las prestaciones del K6 y el CELERON en aplicaciones ofimáticas, aunque es superado por el K6-2, la nueva estrella del zócalo 7.

Este procesador es una muy buena alternativa de bajo coste, especialmente si queremos conservar nuestra placa base, pues muchas placas de una antigüedad media con soporte MMX también admiten el voltaje de 2,9V.

MEDIAGX

Este es un procesador muy interesante diseñado para ordenadores de muy bajo coste.

El MEDIAGX se compone de dos chips, el procesador en sí mismo, que también integra las funciones gráficas y otro chip encargado de las funciones de sonido y las propias del chipset de la placa base. El procesador gráfico está en el propio procesador y utiliza la memoria RAM para almacenar datos.

Se ofrece en velocidades iniciales de 133MHz, 150MHz, 166MHz, 180MHz y 200MHz e integra una caché unificada de nivel 1 de 16KB.

Sus prestaciones son similares a las de un Pentium Clásico, pero su bajo rendimiento en operaciones de coma flotante y programas 3D lo hacen interesante sólo por su muy bajo precio.

El problema de este procesador es que debe estar integrado en la placa base, y por tanto no se puede actualizar. Puede que empecemos a verlo en ordenadores portátiles de bajo coste o en puestos de trabajo en una red, pero no se recomienda como ordenador doméstico.

Elementos de Arquitectura y Seguridad Informática

Recientemente se ha presentado una versión del MediaGX a 233MHz que pronto empezaremos a ver en dispositivos para WINDOWS CE.

MXI

Es la nueva generación del procesador MEDIAGX, siguiendo con la tendencia de la integración, con dos chipsets: el primero, el procesador, que incluye el controlador gráfico; segundo, y el chipset propiamente dicho, que incluye el controlador de sonido.

En esta nueva versión, el MXI incorporará controlador gráfico 2D y 3D, instrucciones MMX y 64KB de caché de primer nivel, y se presentará en versiones PR-300 y PR-400.

IDT

CENTAUR TECHNOLOGY INC., subsidiaria de INTEGRATED DEVICE TECHNOLOGY, INC. (IDT) acaba de lanzar al mercado su primer procesador, caracterizado por un bajo coste, bajo consumo de energía y totalmente compatible con las placas base y chipsets que existen actualmente en el mercado.

WINCHIP C6

Este procesador es compatible con las placas base y chipsets que existen actualmente en el mercado, pues funciona a 3,3V o 3,5V.

El secreto de este procesador es su diseño no super-escalar, parecido al del 486, pero al utilizar el bus de Pentium de 64 bits, una caché de 64KB y un diseño de canal de transferencia de datos avanzado, consigue unas prestaciones similares a las de un Pentium.

Se presenta en velocidades de 150-200MHz, pero sus prestaciones son inferiores, debido a un floja unidad de coma flotante (coprocesador matemático) y la ausencia de instrucciones MMX. Su comportamiento en aplicaciones ofimáticas es bastante bueno, pero su rendimiento desciende ostensiblemente en aplicaciones multimedia.

Este es un procesador adecuado para equipos portátiles de bajo coste o para ordenadores que se utilizan para tareas sencillas. No es un procesador adecuado para un equipo multimedia.

WINCHIP C6 +

Este nuevo procesador de IDT, lanzado en el año 1998, mejora la unidad de coma flotante del C6 y añade instrucciones MMX y la especificación 3DNow! del AMD K6-2 con 53 nuevas instrucciones.

Se presenta en versiones de 200MHz, 225MHz y 240MHz y es compatible con el Zócalo 7, presente en todas las placas para Pentium y en las Super 7.

WINCHIP 2-3D

IDT acaba de anunciar para el año 1999 un nuevo procesador, el WINCHIP 2-3D, con 64KB de caché de nivel 1 y soporte de las instrucciones 3DNow! licenciadas por AMD, que nos suena revolucionario (o anticuado, según de mire) para lo que se estila hoy en día.

Primera novedad, frente a toda la competencia, nada de voltajes duales: este procesador puede funcionar a 3'52V o a 3'3V, es decir, funciona en cualquier placa Pentium Zócalo 7 (incluso las primeras con el chipset 430FX) o en las nuevas Super 7 ¡y sin calentarse en exceso!.

El bus de este procesador es de 60,66, 75, 83 y 100MHz (los dos primeros los hay en todas las placas con Zócalo 7, e incluso en algunas los dos siguientes, pero una placa Super 7 los soporta todos) y el multiplicador es de 2'5x, 3x o 3'5x (también en muchas las placas base Zócalo 7 y Super 7).

Lo único que nos hace falta por último es una actualización de la BIOS que soporte el nuevo procesador.

Este procesador se presentará en versiones de 225MHz (bus de 75MHz), 233MHz (bus de 66MHz), 240MHz (bus de 60MHz), 250MHz (bus de 83MHz), 266MHz (bus de 66MHz) y 300MHz (bus de 75 y 100MHz).

¡Algo falla! NO. Seleccionando en la placa, por ejemplo, 2x obtendríamos en el procesador 2'5x. Curioso, ¿verdad?

PRESTACIONES: podemos equipararlas a las del K6 (no el K6-2) a igual velocidad en aplicaciones ofimáticas, aunque supera a éste en juegos que soporten las instrucciones 3DNow!

A continuación se muestra una tabla con las características principales de los últimos micros presentados por Intel, AMD y Cyrix, y algunas de las proyecciones para el futuro cercano.

Tabla III-1. Tabla Comparativa del Pentium y sus similares

Elementos de Arquitectura y Seguridad Informática

Procesador	AMD K5	AMD K6	Cyrix 6x86MX	Intel Pentium MMX	Intel Pentium II	Intel Deschutes	Intel Tillamook
Interfase	Socket-7	Socket-7	Socket-7	Socket-7	Slot-1	Slot-2	Socket-7
Cache de Datos L1	16KB	32KB	64KB (unified)	16KB	16KB		16KB
Cache de Instrucciones L1	8KB	32KB	N/A	16KB	16KB		16KB
Cache L2	0KB	0KB	0KB	0KB	256KB/512KB	512KB/1024KB/2048KB	0KB
Branch Targeting Buffer Entries	128	8192	1024	256	512	512	256
Velocidad del Reloj	75/90/100/116.5	166/200/233	133/150/166/188	166/200/233	233/266/300	350/400/450/500/550+	266+
PR Rating	PR100/120/133/166	N/A	N/A	N/A	N/A	N/A	N/A
Velocidad del Bus (Oficial)	50/60/66MHz	66MHz	66/75MHz	66MHz	66MHz	66/100MHz	66MHz
Velocidades de Reloj Futuras		250/266/300+	225/233/266		333/350/400/450+	600+	300+
Velocidades del Bus Futuras	None	83/100MHz	83MHz	None	100MHz	150/300MHz	100MHz

Voltaje del Nucleo	3.3/3.52v	2.9/3.2v	2.9v	2.8v	2.8v	2.5v	2.5v
Voltajes Futuros	N/A	2.7/2.5/2.1v	2.5/2.7v		2.5/2.1v	2.1/1.8v	2.1v
Tamaño de Fabricación	0.35 micron	0.30 micron	0.35 micron	0.35 micron	0.35 micron	0.28 micron	0.28 micron
Tamaños Futuros	N/A	0.25 micron	0.25 micron	N/A	0.28 micron	0.25/0.18 micron	0.25 micron

La secuencia de desarrollo a partir del Pentium fue como sigue: Pentium, Pentium Pro, Pentium MMX y Pentium II. Pero el propio Pentium Pro fue un diseño totalmente nuevo, presentando características muy superiores al Pentium.

El Pentium MMX presentó ya algunas características superiores a sus antecesores, entre ellas las siguientes:

Cache L1 de 32 KB, el doble del empleado por el Pentium y por el Pentium Pro.

Fue el primer procesador en emplear la alimentación de voltaje dividida, con el nucleo alimentándose con 2.8v, lo que lo hace un procesador muy interesante para las portátiles.

Introdujo cambios en su arquitectura que balancearon el comportamiento del mismo.

A continuación se muestran algunos resultados del Pentium MMX:

Tabla III-2

Segunda Generación Intel Pentium MMX Series Microprocessor			
Name	Clock Speed	Bus Speed x Multiplier	Fab. Size
Intel Pentium MMX 233	233MHz	66 MHz x 3.5	0.35 micron
Tercera Generación Intel Pentium MMX Series Microprocessor			
Chip	Clock Speed	Bus Speed x Multiplier	Fab. Size
Intel Tillamook 266	266MHz	66 MHz x 4.0	0.28 micron
Intel Mobile Tillamook 233	233MHz	66 MHz x 3.5	0.28 micron
Intel Mobile Tillamook 266	266MHz	66 MHz x 4.0	0.28 micron

Intel Pentium MMX - Wintune 97

Tabla III-3

Chip	Millones de Instrucciones	Millones de Instrucciones en
	por segundo (entero)	Punto Flotante por segundo (FPU)
PMMX-233	435	133
PMMX-262.5	499	149
PMMX-290.5	537	166

El Pentium II introdujo a su vez, nuevas diferencias (Figura III.1).

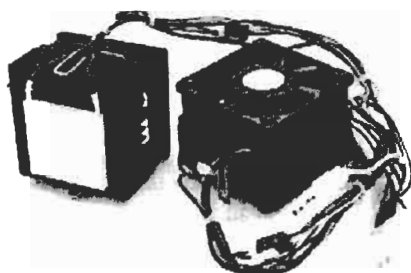


Figura III.1. Microprocesador Pentium II

Contenido en una tarjeta, que se conecta a una ranura especial conocida como SEC Slot-1 (Single Edge Connector Slot-1). Doble bus independiente (DIB - Dual Independent Bus). Introducido originalmente con el Pentium Pro, permite que el CPU y el cache L2 operen simultáneamente con velocidades de reloj iguales, o muy cercanas. Alta generación de calor que requiere, simultáneamente, un disipador de calor y un ventilador.

Soporte superior para multiprocesamiento.

A continuación se muestran algunas características de las generaciones de Pentium II y algunos de sus resultados.

Tabla III-4

Primera Generación Intel Pentium II MMX			
Chip	Clock Speed	Bus Speed	Fab. Size
		Multiplier	
Intel Pentium II MMX 233	233MHz	66 MHz x 3.5	0.35 micron

Intel Pentium II MMX 266	266MHz	66 MHz x 4.0	0.35 micron
Intel Pentium II MMX 300	300MHz	66 MHz x 4.5	0.35 micron

Tabla III-5

Segunda Generación Intel Pentium II MMX			
Chip	Clock Speed	Bus Speed Multiplier	Fab. Size
Intel Pentium II MMX 333	333MHz	66 MHz x 5.0	0.25 micron
Intel Pentium II MMX 350	350MHz	100 MHz x 3.5	0.25 micron
Intel Pentium II MMX 400	400MHz	100 MHz x 4.0	0.25 micron
Intel Pentium II MMX 450	450MHz	100 MHz x 4.5	0.25 micron

Tabla III-6

Primera Generación Intel Mobil Pentium II MMX			
Chip	Clock Speed	Bus Speed Multiplier	Fab. Size
Intel Pentium II MMX 233 - "Lite"	233MHz	66 MHz x 3.5	0.25 micron
Intel Pentium II MMX 266 - "Lite"	266MHz	66 MHz x 4.0	0.25 micron
Intel Pentium II MMX 300 - "Lite"	300MHz	66 MHz x 4.5	0.25 micron

El Overclocking

Que es el Overclocking?. La palabra overclocking hace referencia a **subir la velocidad de reloj de algo por encima de la nominal**; por ejemplo, hacer funcionar un microprocesador que nos han vendido como "de 300 MHz" a una velocidad de 333 MHz. Evidentemente, esto produce un aumento en las prestaciones, aunque también **puede implicar ciertos riesgos relativamente serios para el equipo**, especialmente si no sabemos bien qué estamos haciendo.

Elementos de Arquitectura y Seguridad Informática

Muchos se preguntarán cómo es posible esta "magia" de acelerar la velocidad de algo por encima de la teóricamente correcta. El motivo es que todos los aparatos electrónicos se construyen con unos ciertos **márgenes de seguridad** en cuanto a sus condiciones de trabajo. En el caso concreto de los microprocesadores, que será de quienes trataremos en este artículo, puede afirmarse que en líneas generales todos los microprocesadores de una misma gama se construyen basándose en un diseño idéntico, y sólo posteriormente se clasifican y marcan como de una velocidad determinada.

¿Cómo?!! ¿Que Intel nos engaña? ¿Es que el Pentium MMX de 233 MHz es idéntico al otro de 166 MHz que vendían? No, tampoco es eso. Sencillamente, aunque esos dos micros comparten un diseño idéntico, Intel **nos asegura** que el modelo de 233 MHz puede soportar dicha velocidad a la perfección, mientras que no se hace responsable de que el modelo de 166 MHz tolere nada por encima de dicha velocidad. Pero la realidad es que tal vez sea posible que sí soporte más, y en esa posibilidad basaremos nuestros esfuerzos. Consiste en forzar algunos componentes del ordenador para que den mayor rendimiento del previsto por el fabricante, haciéndolos trabajar en unas condiciones para las que no fueron diseñados. Esta práctica puede realizarse a propósito o bien haber sido víctima de un engaño, según; en cualquier caso, entraña riesgos para el micro overclockeado. Insisto: entraña riesgos para el micro. Los micros de una misma clase nacen, en líneas generales, todos iguales. Luego se prueban y se les clasifica con tal o cual velocidad, según la demanda del mercado y lo que se ha comprobado que resisten sin fallo alguno.

Esto quiere decir que muchos micros pueden ser utilizados a más velocidad de la que marcan, aunque fuera de especificaciones y por tanto de garantía. Las consecuencias negativas son tres:

que no funcione a más velocidad de la marcada (pues nada, se le deja como viene y en paz);

que se estropee (rara vez pasa si se sube de manera escalonada y vigilando si falla);

que funcione pero se caliente (pasará SIEMPRE; al ir más rápido, genera más calor).

El componente al que habitualmente se le aplica esta técnica es el procesador, pero también es útil para acelerar la memoria, las tarjetas de video y los dispositivos PCI, entrando en este último grupo el acceso a los discos, ya que sus controladoras, tanto las IDE como las SCSI van conectadas ese bus.

La técnica más común empleada en el procesador, aunque no la única es hacerlo trabajar a más frecuencia de la que marca. Por ejemplo un Pentium MMX a 166 lo usamos como si fuera uno a 233.

En cuanto al resto de los componentes, la operación más común es subir la frecuencia de la placa base, que es la que surte de datos a las memorias y a las tarjetas PCI, incluyendo las tarjetas de video.

Además, también se pueden forzar los procesadores de las tarjetas gráficas, y para ello existen programas especializados.

Entonces, si esto es posible, ¿Porque no lo hace todo el mundo?

Uno de los principales problemas radica en que cuando un componente electrónico funciona a una velocidad más alta, **produce una cantidad de calor más elevada**. Este calor puede dañar al componente de diversas formas, desde acortar su vida útil (por un efecto físico llamado "electromigración") hasta sencillamente quemarlo, pasando por el caso más habitual: que funcione, pero no de forma estable. En cualquier caso, **el riesgo es mínimo si se procede con prudencia**, siguiendo los pasos con atención y realizando las pruebas poco a poco. Por ejemplo, nada de empezar por un "subidón" de 100 MHz, mejor primero un poco, luego otro poco más, luego otro poco... y entre prueba y prueba, comprobar la estabilidad del sistema, el calor generado, etc. Y como hemos comentado, la realización de estas prácticas implica la pérdida de la garantía del producto, lo cual es lógico desde el punto de vista del fabricante y para nada censurable. Como en casi todo en la vida, la diferencia entre el éxito y el fracaso radica en saber bien lo que se hace.

El Overclocking tiene sus riesgos, aunque es difícil que lleguemos a "quemar" algún componente, si que seguramente lo que haremos es acortar su vida. Además hay que contar con que normalmente hay que emplear técnicas para contrarrestar la mayor disipación de calor que ello conlleva, y que requiere de conocimientos y algo de dinero.

También hay que decir que normalmente los procesadores (sobretudo los de Intel) tienen una vida muy por encima de la que vamos a poder usar. Es decir, hoy en día un procesador 8088 prácticamente no nos servirá para nada, aunque se encuentre en óptimas condiciones.

Además, al final, cuando un procesador ya no "tira" porque el software cada vez le exige más, el Overclocking es prácticamente lo único que nos queda, si no podemos hacer el esfuerzo de comprar un procesador nuevo.

```
CPU Name Is : Intel Celeron MMX
CPU Operating Speed : User Define
- Ext. Clock (PCI) : 75MHz(1/3)
- Multiplier Factor : x6
- SEL100/66# Signal : Low
- AGPCLK/CPULCK : 1/1
- Speed Error Hold : Disabled

CPU Power Supply : CPU Default
- Core Voltage : 2.00v
```

Figura III.2. Vista del SETUP para la configuración del Overclocking

Y por último, dependiendo de los tipos de procesador, y del modelo en concreto que nos haya tocado, algunos realmente no se pueden forzar, o en cantidad

Elementos de Arquitectura y Seguridad Informática

mínima, ya que simplemente se niegan a trabajar, o provocan "cuelgues" o reinicios espontáneos, o en casos muy remotos incluso puede peligrar la vida de nuestros datos. Las consecuencias positivas, que tenemos un micro más rápido gratis. Si desea arriesgarse, coja el manual de su placa y siga estos consejos para hacer overlocking con un micro: usar un disipador y un BUEN

VENTILADOR; subir la velocidad gradualmente, nunca en saltos de más de 33 MHz; en ocasiones hará falta subir unas décimas el voltaje al que trabaja el micro para conseguir estabilidad, aunque no es lo deseable por aumentar el calor a disipar; estar atentos a cualquier fallo de ejecución, que significará que el micro no está muy estable. A este respecto, Windows 9x y NT son mucho más exquisitos que el viejo, adorable y tolerante DOS; no pedir imposibles. Subir 33 MHz un Pentium clásico ya está bien; subirlo 50 ó 66 MHz es una pasada bastante arriesgada; subirlo 100 MHz es una idiotez condenada al fracaso y a quemar el micro.

Desgraciadamente, en los últimos tiempos los fabricantes de microprocesadores (en especial Intel) han tomado consciencia de lo común que se estaba volviendo esta técnica y han decidido ponerle un cierto freno, por lo que muchos micros recientes (entre ellos los Pentium II y Celeron más modernos) tienen fijo el multiplicador del bus a una única opción; por ejemplo, los Celeron a 333 MHz suelen poder usar únicamente un multiplicador x5. Pero no debe preocuparse, aparte de utilizar un multiplicador mayor, Existe otra forma interesante de hacer overlocking: subir la velocidad externa (o de bus) a la que se comunica el micro con la placa, por ejemplo poniendo uno de esos Celeron de 333 MHz con multiplicador x5 fijo a $(75 \times 5 = 375 \text{ MHz})$ en vez de a los (66×5) normales. Eso sí, de esta forma los problemas de estabilidad pueden darlos otros componentes que trabajan a la velocidad del bus o una fracción de ésta, como las tarjetas de expansión PCI y AGP o la memoria, sobre todo si son de baja calidad...

Aunque esto no tiene porqué ser un problema: podríamos no ya variar la velocidad total del micro, sino usar ambos sistemas a la vez, por ejemplo poniendo un micro de 150 MHz a (75×2) en vez de a $(60 \times 2,5)$ (sólo en micros con el multiplicador no fijo, claro), con objeto de obtener un rendimiento mayor al acelerar los componentes anteriormente citados. Además, en este caso apenas estamos variando las condiciones de trabajo del micro, que suele ser el factor más conflictivo (exceptuando algunas tarjetas AGP que se calientan como demonios).

Bueno, está avisado de lo bueno y lo malo. Por cierto, la explicación se ha dado para Pentium o superiores; para 486 es válida, aunque procure subirlas menos (de 33 a 40 MHz, o de 66 a 80, por ejemplo). Hacer overlocking con un 386 o inferior es más complicado y no merece la pena.

Relaciones de multiplicacion del microprocesador

¿Cómo funciona un micro?

A partir de ahora vamos a centrarnos en las posibilidades que existen para acelerar la velocidad del micro, para lo cual inexcusablemente debemos explicar un poco cómo funcionan estos aparatos.

El microprocesador, también llamado "la CPU", es el cerebro del ordenador. Es el chip más versátil, el que se encarga de la mayor parte de los cálculos y, generalmente, el más rápido. Evidentemente, cuanto mayor sea la velocidad a la que debe funcionar un chip, más difícil y caro será fabricarlo; por ello, **el micro funciona a una velocidad que es un múltiplo de la de la placa base**, de forma que los otros componentes (el chipset de la placa base, la memoria, las tarjetas de expansión...) pueden mantener un precio mucho más ajustado y utilizarse con muchos micros distintos, con sólo ajustar esos **multiplicadores**.

Por tanto, el micro funciona a dos velocidades, una interna y otra externa o de comunicación con la placa base (la del llamado **bus de sistema**, externo, de memoria o "FSB" en Pentium II-III y similares). Así, mientras la placa base funciona por ejemplo a 66 MHz, el micro funcionará a 200 MHz mediante el uso de un multiplicador 3x, o a 233 MHz mediante un 3,5x.

Posibilidades para el overclocking

El ritmo creciente de las distintas tecnologías en nuestro mundo actual no admite comparación alguna con ninguna otra. Los cambios sustanciales se suceden continuamente, sin existir ni siquiera un simple mes en el cual no ocurran cosas de importancia. Una de las áreas donde esto se refleja fielmente, es la concerniente al hardware de las microcomputadoras, principalmente su componentes esenciales, el CPU.

Teniendo en cuenta la teoría de aumentar la velocidad del microprocesador, tenemos 3 diferentes posibilidades para realizar el overclocking:

(1) Subir el multiplicador del micro.

Mediante este método variaremos sólo la velocidad interna del micro, mientras que la externa permanecerá constante. De esta forma, **el único elemento que sufre es el micro**, mientras que los demás aparatos trabajan a su velocidad normal.

Deberemos estudiar el manual de la placa base y ver cómo se realiza el cambio del multiplicador; en el caso más habitual se hará mediante unos pequeños microinterruptores denominados jumpers, aunque en las placas base más modernas se realiza por software, generalmente dentro de la BIOS (en esto las placas ABIT fueron las primeras). Incluso, en el peor de los casos, puede que la placa detecte automáticamente las características teóricas del micro y no nos deje configurarlas a mano... como sucede en algunas placas base fabricadas por Intel.

Otro problema que se da actualmente es que **casí todos los micros Intel a partir del Pentium II de 300 MHz** (incluyendo los Pentium III y Celeron "Mendocino"), así como algunas series anteriores, **tienen el multiplicador limitado a unos valores concretos o fijo a un único valor**, por ejemplo 4x para un Pentium II de 400 MHz

Elementos de Arquitectura y Seguridad Informática

(4x100). En tal caso, y si no tenemos un micro AMD (que tienen el multiplicador libre), deberemos probar a:

(2) Subir la velocidad del bus.

Haciendo esto aumentaremos la velocidad tanto del microprocesador como de los demás elementos del ordenador (la placa base, la memoria, las tarjetas de expansión...). De nuevo, se configurará mediante jumpers o en la BIOS.

Tabla III-7

	Micro normal (5x66 = 333 MHz)	Micro overcloveado (5x75 = 375 MHz)
Memoria	66 MHz	75 MHz
Bus AGP	66 MHz	75 MHz
Bus PCI	33 MHz	75/2 = 37,5 MHz 75/3 = 25 MHz
Bus ISA	8 MHz	9 MHz

Por ejemplo, la configuración "oficial" de un Pentium II de 333 MHz es 5x66; si ponemos un bus de 75 MHz, el overlocking tendría los siguientes efectos:

Observe cómo la velocidad de los diferentes elementos suele estar relacionada con la de bus (o externa) del micro:

en el caso de la memoria, suele ser igual a la de bus (excepto en algunas placas, sobre todo en algunas que emplean chipsets VIA);

el bus AGP suele funcionar a la velocidad de bus o a los 2/3 de ésta; en placas de ultimísima generación, también a 1/2;

el bus PCI suele poderse seleccionar a 1/2, 1/3 e incluso 1/4 de la velocidad de bus;

el bus ISA apenas da problemas, y varía muy poco.

Al sufrir tantos elementos el overlocking, los posibles fallos se multiplican, ya que basta con que un elemento falle para que no tengamos éxito. Sin embargo, **si lo conseguimos, el aumento de prestaciones será muy grande**, ya que estamos acelerando casi todos los elementos del PC, y no nos afectarán las limitaciones impuestas por el fabricante del micro (al menos por ahora...).

(3) Cambiar el multiplicador y la velocidad del bus.

Es un método que puede dar mucho juego, aunque de nuevo sólo realizable con micros sin multiplicador fijo. Podemos hacer auténticas maravillas, e incluso conseguir acelerar el ordenador sin variar la velocidad interna del micro para que

no sufra, por ejemplo cambiando un Pentium 150 de 2,5x60 a 2x75, lo que aceleraría el bus PCI y la memoria sin riesgo para el micro.

Para lograr elevar las prestaciones de los Pentium, se ha empleado una técnica de multiplicación del reloj (overclocking), técnica que consiste aumentar uno o los dos aspectos siguientes:

Relación de multiplicación del Reloj

Velocidad del Bus

La tabla que sigue muestra esta técnica como se ha empleado.

Tabla III-8

CPU	Veloc. Del Bus	Multiplicador del Reloj	Opción 1	Opción 2
AMD K5 PR/75+ @ 75MHz	50MHz	1.5x	75 x 1.5 = 113MHz	66 x 1.5 = 100MHz
AMD K5 PR/90+ @ 90MHz	60MHz	1.5x	75 x 1.5 = 113MHz	66 x 1.5 = 100MHz
AMD K5 PR/100+ @ 100MHz	66MHz	1.5x	75 x 1.5 = 113MHz	N/A
AMD K5 PR/133+ @ 100MHz	66MHz	1.5x	75 x 1.5 = 113MHz	N/A
AMD K5 PR/166+ @ ~116MHz	66MHz	(Interno) 2.5x	N/A	75 x 1.5 = 112.5MHz
AMD K6 PR2/166MHz	66MHz	2.5x	83 x 2.5 = 210MHz	83 x 2.0 = 166MHz
AMD K6 PR2/200MHz	66MHz	3.0x	83 x 2.5 = 210MHz	75 x 3.0 = 225MHz
AMD K6 PR2/233MHz	66MHz	(Interno) 1.5x	83 x 3.0 = 250MHz	75 x 3.5x = 262.5MHz
Cyrix 6x86 PR90+ @ 80MHz	40MHz	2.0x	50 x 2.0 = 100MHz	N/A
Cyrix 6x86 PR120+ @ 100MHz	50MHz	2.0x	55 x 2.0 = 110MHz	N/A
Cyrix 6x86 PR133+ @ 110MHz	55MHz	2.0x	60 x 2.0 = 120MHz	N/A

Elementos de Arquitectura y Seguridad Informática

CPU	Veloc. Del Bus	Multiplicador del Reloj	Opción 1	Opción 2
Cyrix 6x86 PR150+ @ 120MHz	60MHz	2.0x	66 x 2.0 = 133MHz	N/A
Cyrix 6x86 PR166+ @ 133MHz	66MHz	2.0x	75 x 2.0 = 150MHz	N/A
Cyrix 6x86 PR200+ @ 150MHz	75MHz	2.0x	83 x 2.0 = 166MHz	N/A
Intel Pentium 100MHz	66MHz	1.5x	83 x 1.5 = 125MHz	75 x 1.5 = 112.5MHz
Intel Pentium 120MHz	60MHz	2.0x	83 x 1.5 = 125MHz	66 x 2.0 = 133MHz
Intel Pentium 133MHz	66MHz	2.0x	83 x 2.0 = 166MHz	75 x 2.0 = 150MHz
Intel Pentium 150MHz	60MHz	2.5x	83 x 2.0 = 166MHz	75 x 2.0 = 150MHz
Intel Pentium 166MHz	66MHz	2.5x	83 x 2.5 = 208.3MHz	83 x 2.0 = 166MHz
Intel Pentium 180MHz	60MHz	3.0x	83 x 2.5 = 208.3MHz	83 x 2.0 = 166MHz
Intel Pentium 200MHz	66MHz	3.0x	83 x 3.0 = 250MHz	83 x 2.5 = 210MHz
Intel Pentium 233MHz	66MHz	3.5x	83 x 3.0 = 250MHz	N/A
Intel Pentium II - 233MHz	66MHz	3.5x	66 x 4.0 = 266MHz	N/A

¿Cuánto puede overclockearse un micro?

Depende del micro. No, no es sólo una forma de "escaquearme" de responder, es una realidad: cada micro es un mundo, y es distinto a todos los demás. Incluso dos micros del mismo modelo, de la misma fábrica y hasta de la misma serie pueden tener distinta tolerancia al overclocking, y no hay forma de saberlo a priori.

Sin embargo, sí pueden darse unas cuantas indicaciones:

Tabla III-9

Tipo de micro	Descripción del micro original	Notas - Consejos
Pentium clásicos (no MMX)	Bus de 50/60/66 MHz Multiplicador libre	Permiten muchas posibilidades, cambiando el bus y/o el multiplicador; pocas placas de esta época admitirán la velocidad de 75 MHz
Pentium MMX	Bus de 66 MHz Multiplicador libre	Permiten muchas posibilidades, cambiando el bus y/o el multiplicador, aunque éste estaba limitado en algunas series
AMD K5	Bus de 50/60/66 MHz Multiplicador fijo	Limitados a cambiar la velocidad del bus
AMD K6	Bus de 66 MHz Multiplicador libre	Permiten muchas posibilidades, cambiando el bus y/o el multiplicador; existen dos modelos de K6 a 233 MHz, uno de ellos funciona a 3,2 V, por lo que se calienta demasiado
AMD K6-2	Bus de 66/95/100 MHz Multiplicador libre	Permiten muchas posibilidades, cambiando el bus y/o el multiplicador; los escasos modelos de más de 300 MHz que emplean bus de 66 MHz son muy poco recomendables
Cyrix 6x86/M2	Bus de 50/55/60/66/75 MHz Multiplicador limitado	Aunque no todos permiten cambiar el multiplicador, las posibilidades son bastantes, pero algunas series tienen un voltaje excesivo; en general, tal vez sean algo delicados
Pentium II hasta 333 MHz	Bus de 66 MHz Multiplicador ¿?	Muy buenos o muy malos para el overclocking, dependiendo de las posibilidades del multiplicador (fijo a partir del de 300 MHz) y de las características de la placa

Elementos de Arquitectura y Seguridad Informática

Tipo de micro	Descripción del micro original	Notas - Consejos
Pentium II de 350 MHz o más, primeros Pentium III	Bus de 100 MHz Multiplicador fijo	Todo dependerá de las características de la placa (algunas ofrecen buses de 105, 110... y hasta 133 MHz, otras sólo de 100 MHz)
Pentium III modernos (núcleo "Coppermine")	Bus de 100 ó 133 MHz Multiplicador fijo	Todo dependerá de las características de la placa; en todo caso, permiten overclockings elevados gracias a su reducido voltaje
Celeron sin caché	Bus de 66 MHz Multiplicador libre	De lo mejor para overclocking, pero la falta de caché le ralentiza en muchas tareas (aunque en juegos va bien)
Celeron "A" (con 128 KB de caché o "Mendocino")	Bus de 66 MHz Multiplicador fijo	De lo mejor para overclocking, pese al multiplicador fijo. Suele admitir bien pasar de 66 a 75 MHz, e incluso el modelo de 300 MHz es famoso por funcionar (a veces) a ¡450 MHz!!
AMD K7 Athlon	Bus de 200 MHz (100x2) Multiplicador libre	Fantástica capacidad de overclocking, pero para aprovecharla al máximo debe abrirse su carcasa y soldar, o bien utilizar pequeñas placas de circuito adicionales ("gold fingers")

A lo que se puede añadir que si lo que desea es un ordenador nuevo para hacer overclocking (aunque ninguna garantía le cubrirá los posibles daños), coloque memoria SDRAM de 133 MHz (PC133), preferiblemente de marca. A la hora de hacer overclocking o de actualizarse, lo agradecerá.

La refrigeración

Como decíamos, el overclocking, exitoso o no, SIEMPRE produce calor. Este calor es uno de los principales enemigos de todo aparato electrónico, por lo que debemos ocuparnos de eliminarlo de nuestro sistema. Muy pocos micros son capaces de soportar 70°C sin volverse terriblemente inestables o empezar a "quemarse".

Primero debemos refrigerar el componente en cuestión, en general el micro, aunque la tarjeta gráfica también puede calentarse bastante. Para ello, existe un disipador de calor sobre el micro, que absorbe el calor por su superficie y lo expulsa, ayudado por un ventilador para evitar que se estanque ese aire caliente cerca del micro.

Como es lógico, **cuanto mayores sean el disipador y el ventilador, mejor**. Existen ventiladores que permiten controlar su velocidad de rotación o la temperatura del disipador con el que están en contacto, lo que es algo muy importante. No es nada

raro que un ventilador estándar, que suelen ser de una calidad bastante mediocre, se quede atascado sin avisar y quemé el micro (uno de los motivos por los que no se debe dejar solo un ordenador overclockeado hasta saber si funciona bien al 100%).

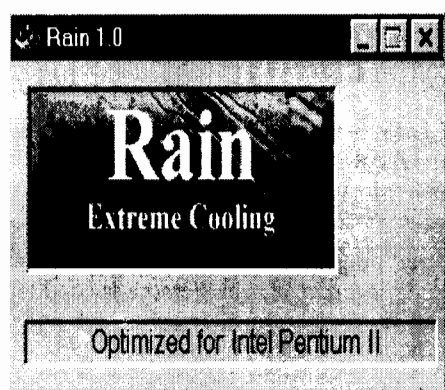


Figura III.3. Vista de un Software que permite la refrigeración del microprocesador.

Otros dispositivos que pueden ayudar mucho en un overclocking son las **células Peltier**. Estos curiosos aparatos son unas láminas que, al ser atravesadas por la corriente eléctrica, hacen que una de sus caras se enfríe bastante, mientras que la otra se calienta (también bastante, por lo que en esa cara debe seguir colocándose un disipador y un ventilador). Estos aparatos son muy eficaces, pero lo malo es que consumen mucha potencia eléctrica.

De cualquier forma, sea cual sea el método para refrigerar el ventilador, **no servirá de nada si no expulsamos el calor al exterior de la carcasa del ordenador.**

Tenga en cuenta que el disipador y el ventilador no hacen que el calor desaparezca, sólo lo trasladan de sitio, pero tan dañino es cerca del micro como acumulándose dentro de la carcasa sin poder salir...

Para que la refrigeración sea perfecta, lo ideal es tener un ventilador que introduzca aire frío en la carcasa y otro que lo expulse. En un equipo normal, la fuente de alimentación suele sacar el aire caliente, pero no suele haber un ventilador de entrada. Así que no será ninguna tontería instalar un ventilador en la parte frontal de nuestro ordenador.

En cualquier caso, tenga en cuenta dos puntos: uno, que el aire caliente sube, así que la salida de aire debe estar arriba (NUNCA situada debajo de la entrada de aire frío); y dos, que existen pocos esquemas de ventilación tan efectivos y baratos como **abrir la carcasa del ordenador**. No es muy bonito (bueno, hay gustos para todo), pero funciona muy bien.

Refrigeración por software

Elementos de Arquitectura y Seguridad Informática

Este otro método para enfriar los micros consiste en aprovechar una serie de **órdenes de ahorro energético** presentes en todos los micros desde la época de los Pentium; mediante estas órdenes ponemos a descansar aquellas partes del micro que no están trabajando en este momento, reduciendo mucho la temperatura del micro.

Desgraciadamente, el sistema tiene una limitación insalvable: cuando el micro se utiliza al máximo de su potencia en todo momento, la refrigeración no puede realizarse; por ello, sería muy poco eficaz si por ejemplo estamos jugando sin parar a un juego 3D sumamente complejo.

De cualquier modo, los programas aprovechan tiempos muertos bastante más pequeños que décimas de segundo, así que siempre pueden ser útiles, por lo menos como apoyo a un buen ventilador. De los muchos que hay, recomendaríamos el veterano **Rain** (Figura III.3), que es de muchísima eficacia y estabilidad.

Algunas recomendaciones

Para que un overclocking sea exitoso, conviene seguir estas pequeñas reglas:

Tenga muy claro lo que está haciendo ANTES de hacerlo. Para qué engañarnos, esto puede ser peligroso (principalmente para su economía, si llega a quemar el micro).

Sea prudente, vaya con calma. Desconecte el ordenador de la corriente (salvo que la configuración se haga en la BIOS, claro), descárguese de electricidad estática y compare cuidadosamente las configuraciones de los jumpers del manual con las que usted selecciona.

Suba la velocidad gradualmente, poco a poco, y compruebe cada vez que el ordenador funciona bien y de forma estable, para lo cual nada mejor que ejecutar Windows 9x/NT y un par de juegos exigentes durante un rato.

Nunca deje encendido sin vigilancia un sistema overlockeado de cuya estabilidad no esté seguro al 100%, puede que el micro empiece a freírse y se tenga que enterar por el humo... (es broma, claro)

Si el overclocking no funciona, **intente aislar el fallo**: ¿es el micro? ¿La memoria, tal vez? ¿Alguna tarjeta PCI muy delicada? Una vez aislado, actúe en consecuencia:

- pruebe a seleccionar otra combinación de bus/multiplicador;
- si el problema es un bus (ISA, PCI, AGP), busque en la BIOS si puede seleccionar otros divisores, como 1/3 de la velocidad de la placa para PCI, o 2/3 para AGP;
- si es la memoria, pruebe a cambiar su velocidad (de "Fast" a "Low", o aumentar los "wait states", o pasar de CAS 2 a CAS 3...)

Esté muy pendiente de la temperatura de los componentes, especialmente del micro y de la tarjeta gráfica (las modernas tarjetas AGP se calientan bastante), y **refrigere los componentes lo más posible**. En apartados posteriores trataremos de esto.

Puede subir una o como mucho dos décimas el voltaje del micro para estabilizarlo, pero no es recomendable, ya que implica un riesgo elevado: se producirá bastante más calor, lo que no es NADA bueno.

Sea realista: en algunos casos, subir 33 MHz ya es todo un logro, así que no espere milagros. Después de todo, está consiguiendo duros a 4 pesetas, querer conseguirlos a 3 ya es abusar.

IV. Torres de discos y otros medios de almacenamiento

Disqueteras

A la hora de ampliar nuestros ordenadores nos mueve algo que se puede definir con una palabra clave: necesidad. Necesidades de potencia, versatilidad, rapidez, y cómo no, almacenamiento. El software va tomando continuamente un tamaño mastodónico, y además nuestro trabajo con el ordenador va ocupando cada vez más espacio; curiosamente no basta con un disco duro de gran tamaño, puesto que éste también se va llenando rápidamente.

Todos tenemos datos y programas de los que no queremos o no podemos desprendernos, aún en el caso más que probable de que estos últimos estén desfasados: bases de datos, imágenes y sonidos, documentos, etc. Surge por tanto la necesidad de guardar esa información en algún soporte que nos permita eliminarla de nuestro disco duro y reinstalarla en él cuando sea preciso. El medio removible por excelencia es el disquete de 3 1/2", aunque relacionado con él aflora un insondable misterio, al que nadie ha respondido: ¿cómo es posible que un dispositivo que sólo puede almacenar 1.440 Kilobytes sobreviva durante tantos años en un mundo donde la longevidad se mide en escasos meses, y es rarísimo el software que cabe en un sólo disquete? Queda clara, por tanto, la necesidad de contar con una forma de almacenar la mayor cantidad de datos posible, en un soporte removible. El mercado pone a disposición un extenso catálogo de alternativas; comentaremos los más conocidos y empleados, enumerando sus ventajas e inconvenientes.

Refiriéndonos exclusivamente al mundo del PC, en las unidades de disquette sólo han existido dos formatos físicos considerados como estandar, el de 5 1/4 y el de 3 1/2. En formato de 5 1/4, el IBM PC original sólo contaba con unidades de 160 Kb., esto era debido a que dichas unidades sólo aprovechaban una cara de los disquettes. Luego, con la incorporación del PC XT vinieron las unidades de doble cara con una capacidad de 360 Kb. (DD o doble densidad), y más tarde, con el AT, la unidad de alta densidad (HD) y 1,2 Mb.

El formato de 3 1/2 IBM lo impuso en sus modelos PS/2. Para la gama 8086 las de 720 Kb. (DD o doble densidad) y para el resto las de 1,44 Mb. (HD o alta densidad) que son las que hoy todavía perduran. En este mismo formato, también surgió un nuevo modelo de 2,88 Mb. (EHD o Extra alta densidad), pero no consiguió cuajar.

Discos duros

Los discos duros pertenecen a la llamada memoria secundaria o almacenamiento secundario. Al disco duro se le conoce con gran cantidad de denominaciones como disco duro, rígido (frente a los discos flexibles o por su fabricación a base de una capa rígida de aluminio), fijo (por su situación en el ordenador de manera permanente), winchester (por ser esta la primera marca de cabezas para disco duro). Estas denominaciones aunque son las habituales no son exactas ya que existen discos de iguales prestaciones pero son flexibles, o bien removibles o transportables, u otras marcas diferentes fabricantes de cabezas.

Las capacidades de los discos duros varían desde 10 Mb. hasta varios Gb. en minis y grandes ordenadores. Para conectar un disco duro a un ordenador es necesario disponer de una tarjeta controladora. La velocidad de acceso depende en gran parte de la tecnología del propio disco duro y de la tarjeta controladora asociada al discos duro.

Estos están compuestos por varios platos(Figura IV.1), es decir varios discos de material magnético montados sobre un eje central sobre el que se mueven. Para leer y escribir datos en estos platos se usan las cabezas de lectura/escritura que mediante un proceso electromagnético codifican / decodifican la información que han de leer o escribir. La cabeza de lectura/escritura en un disco duro está muy cerca de la superficie, de forma que casi vuela sobre ella, sobre el colchón de aire formado por su propio movimiento. Debido a esto, están cerrados herméticamente, porque cualquier partícula de polvo puede dañarlos.

Los discos duros se presentan recubiertos de una capa magnética delgada, habitualmente de óxido de hierro, y se dividen en unos círculos concéntricos cilindros (coincidentes con las pistas de los disquetes), que empiezan en la parte exterior del disco (primer cilindro) y terminan en la parte interior (último). Asimismo estos cilindros se dividen en sectores, cuyo número esta determinado por el tipo de disco y su formato, siendo todos ellos de un tamaño fijo en cualquier disco. Cilindros como sectores se identifican con una serie de números que se les asignan, empezando por el 1, pues el numero 0 de cada cilindro se reserva para propósitos de identificación mas que para almacenamiento de datos. Estos, escritos/leídos en el disco, deben ajustarse al tamaño fijado del almacenamiento de los sectores. Habitualmente, los sistemas de disco duro contienen más de una unidad en su interior, por lo que el número de caras puede ser más de 2. Estas se identifican con un número, siendo el 0 para la primera. En general su organización es igual a los disquetes. La capacidad del disco resulta de multiplicar el número de caras por el de pistas por cara y por el de sectores por pista, al total por el número de bytes por sector.

Para escribir, la cabeza se sitúa sobre la celda a grabar y se hace pasar por ella un pulso de corriente, lo cual crea un campo magnético en la superficie. Dependiendo del sentido de la corriente, así será la polaridad de la celda. ara leer, se mide la corriente inducida por el campo magnético de la celda. Es decir que al pasar sobre una zona detectará un campo magnético que según se encuentre magnetizada en un sentido u otro, indicará si en esa posición hay almacenado un 0 o un 1. En el caso de la escritura el proceso es el inverso, la cabeza recibe una corriente que provoca

Elementos de Arquitectura y Seguridad Informática

un campo magnético, el cual pone la posición sobre la que se encuentre la cabeza en 0 o en 1 dependiendo del valor del campo magnético provocado por dicha corriente.

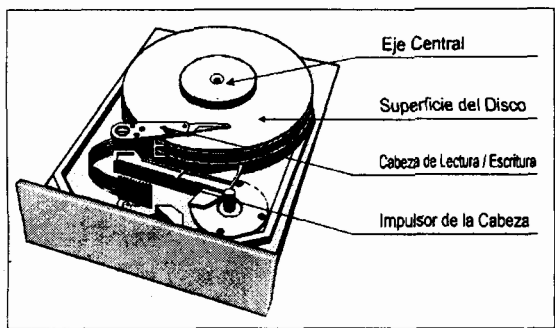


Figura IV.1. Esquema del interior de un disco duro.

Los componentes físicos de una unidad de disco duro son:

- **CABEZA DE LECTURA / ESCRITURA:** Es la parte de la unidad de disco que escribe y lee los datos del disco. Su funcionamiento consiste en una bobina de hilo que se acciona según el campo magnético que detecte sobre el soporte magnético, produciendo una pequeña corriente que es detectada y amplificada por la electrónica de la unidad de disco.
- **DISCO:** Convencionalmente los discos duros están compuestos por varios platos, es decir varios discos de material magnético montados sobre un eje central. Estos discos normalmente tienen dos caras que pueden usarse para el almacenamiento de datos, si bien suele reservarse una para almacenar información de control.
- **EJE:** Es la parte del disco duro que actúa como soporte, sobre el cual están montados y giran los platos del disco.
- **IMPULSOR DE CABEZA:** Es el mecanismo que mueve las cabezas de lectura / escritura radialmente a través de la superficie de los platos de la unidad de disco.

Mientras que lógicamente la capacidad de un disco duro puede ser medida según los siguientes parámetros.

- **CILINDRO:** Es una pila tridimensional de pistas verticales de los múltiples platos. El número de cilindros de un disco corresponde al número de posiciones diferentes en las cuales las cabezas de lectura/escritura pueden moverse.
- **CLUSTER:** Es un grupo de sectores que es la unidad más pequeña de almacenamiento reconocida por el DOS. Normalmente 4 sectores de 512 bytes constituyen un Cluster (racimo), y uno o más Cluster forman una pista.

· **PISTA:** Es la trayectoria circular trazada a través de la superficie circular del plato de un disco por la cabeza de lectura / escritura. Cada pista está formada por uno o más Cluster.

· **SECTOR:** Es la unidad básica de almacenamiento de datos sobre discos duros. En la mayoría de los discos duros los sectores son de 512 Bytes cada uno, cuatro sectores constituyen un Cluster.

Otros elementos a tener en cuenta en el funcionamiento de la unidad es el tiempo medio entre fallos, MTBF (Mean Time Between Failures), se mide en horas (15000, 20000, 30000..) y a mayor número más fiabilidad del disco, ya que hay menor posibilidad de fallo de la unidad. Otro factor es el AUTOPARK o aparcamiento automático de las cabezas, consiste en el posicionamiento de las cabezas en un lugar fuera del alcance de la superficie del disco duro de manera automática al apagar el ordenador, esto evita posibles daños en la superficie del disco duro cuando la unidad es sometida a vibraciones o golpes en un posible traslado.

Parámetros a tener en cuenta:

Capacidad: Aconsejable que sea a partir de 2,1 Gbytes en adelante.

Tiempo medio de acceso: Importante. Este parámetro nos indica la capacidad para acceder de manera aleatoria a cualquier sector del disco.: tiempo que tarda, como media, para desplazarse la cabeza a la posición actual. Este tiempo promedio para acceder a una pista arbitraria es equivalente al tiempo necesario para desplazarse sobre 1/3 de las pistas del disco duro. El antiguo IBM PC/XT utilizaba discos de 80 a 110 milisegundos, mientras que los AT usaban discos de 28 a 40 milisegundos, y los actuales sistemas 386, 486 y PENTIUM[®] usan discos de menos de 20 milisegundos.

Velocidad de Transferencia: Directamente relacionada con el interface.

En un dispositivo Ultra-2 SCSI es de 80 MBytes/seg. mientras que en el Ultra DMA/33 (IDE) es de 33,3 MBytes/seg. en el modo DMA-2. Esta velocidad es la máxima que admite el interface, y no quiere decir que el disco sea capaz de alcanzarla.

Velocidad de Rotación: Tal vez el más importante. Suele oscilar entre las 4.500 y las 7.200 rpm (revoluciones por minuto).

Latencia Promedio : Es el promedio de tiempo para que el disco una vez en la pista correcta encuentre el sector deseado, es decir el tiempo que tarda el disco en dar media vuelta. Velocidad de transferencia : velocidad a la que los datos (bits) pueden transferirse desde el disco a la unidad central. Depende esencialmente de dos factores : la velocidad de rotación y la densidad de almacenamiento de los datos en una pista.

3600 rpm = 1 revolución cada 60/3600 segundos (16,66 milisegundos)

Si calculamos el tiempo de ½ vuelta → Latencia Promedio 8,33 milisegundos

Elementos de Arquitectura y Seguridad Informática

Una comparativa entre un disquete y un disco duro de todos estos Factores mencionados anteriormente sería:

Tabla IV-1

	T.Pista	T.Macceso	Rotación	Latencia	V.Transfrecia
FD 360k	6-12 mls	93 mls	300 rpm	100 mls	125-250 Kb / seg
HD AT 30	8-10 mls	40-28 mls	3600 rpm	8,3 mls	1-5 Mb / seg

El tiempo de búsqueda depende del **tamaño** de la unidad (2", 3"½, 5"¼), del número de **pistas por pulgada** (que a su vez depende de factores como el tamaño de los dominios magnéticos) y de la velocidad y la precisión de los engranajes del cabezal. La latencia depende de la velocidad de **rotación** y equivale a la mitad del tiempo que tarda el disco en describir un giro completo. El rendimiento total también depende de la disposición de los dominios magnéticos, uso de ZBR.

Para mejorar el tiempo de acceso se reduce esa latencia acelerando la rotación del disco o velocidad de eje. Hace unos años todos los discos duros giraban a la misma velocidad unos 3600 rpm, la latencia resultante era de 8,3 milisegundos. Hoy las unidades de disco más rápidas para PC giran a 5400 rpm (un 50% más rápidas) y por tanto su latencia es de 5,6 milisegundos. Algunos discos siguen usando los 3600 rpm para consumir menos energía.

Tabla IV-2

RPM	1 Vuelta cada	Latencia
3600	16,66 mseg.	8,33 mseg.
4500	13,33 mseg.	6,66 mseg.
5400	11,11 mseg.	5,55 mseg.
7200	8,33 mseg.	4,16 mseg.
10000	6,00 mseg.	3,00 mseg.

El trabajar a velocidades elevadas plantea varios problemas: El primer problema es que a esta velocidad la disipación del calor se convierte en un problema. El segundo es que exige a usar nuevos motores articulados pro fluidos para los engranajes, los actuales motores de cojinetes no pueden alcanzar estas velocidades sin una reducción drástica de fiabilidad, se quemarían demasiado rápido.

Además de todas estas características de velocidades y tiempos de acceso de los discos duros existen una serie de técnicas que nos permiten aminorar los accesos a disco así como acelerar las transferencias de datos entre el sistema y el dispositivo en cuestión. Una de las técnicas más conocidas en la informática para hacer esto es la del uso de memorias intermedias, buffers o cachés.

Buffer De Pista: Es una memoria incluida en la electrónica de las unidades de disco, que almacena el contenido de una pista completa. Así cuando se hace una petición de lectura de una pista, esta se puede leer de una sola vez, enviando la información a la CPU, sin necesidad de interleaving.

Cachés De Disco: La memoria caché implementada en el disco es importante, pero más que la cantidad es importante la manera en que ésta se organiza. Por ello este dato normalmente no nos da por sí solo demasiadas pistas. Son normales valores entre 64 y 256 Kb. Pueden estar dentro del propio disco duro, en tarjetas especiales o bien a través de programas usar la memoria central. La gestión de esta memoria es completamente invisible y consiste en almacenar en ella los datos más pedidos por la CPU y retirar de ella aquellos no solicitados en un determinado tiempo. Se usan para descargar al sistema de las lentas tareas de escritura en disco y aumentar la velocidad.

Aparte de la velocidad del disco duro y de la controladora la forma en que se transfieren los datos de ésta a la memoria decide también la velocidad del sistema. Se pueden emplear 4 métodos:

Programed I/O (Pio Mode): La transferencia de datos se desarrolla a través de los diferentes puerto I/O de la controladora que también sirven para la transmisión de comandos (IN / OUT). La tasa de transferencia está limitada por los valores del bus PC, y por el rendimiento de la CPU. Se pueden lograr transferencias de 3 a 4 Mbytes. Con el modo de transferencia PIO 4, que es el método de acceso que actualmente utilizan los discos más modernos, es posible llegar a tasas de transferencia de 16,6 Mbytes / seg.

Memory mapped I/O: La CPU puede recoger los datos de la controladora de forma más rápida, si los deja en una zona de memoria fija, ya que entonces se puede realizar la transferencia de los datos a una zona de memoria del programa correspondiente con la introducción MOV, más rápida que los accesos con IN y OUT. El valor teórico máximo es de 8 Mbytes / seg.

DMA: Es la transferencia de datos desde el disco a la memoria evitando pasar por la CPU. La ventaja de usar el DMA es que se libera al procesador para trabajar en otras tareas mientras las transferencias de datos se realizan por otro lado. El DMA además de ser inflexible es lento, no se puede pasar de más de 2 Mb. por segundo.

Bus Master DMA: En esta técnica la controladora del disco duro desconecta la controladora del bus y transfiere los datos con la ayuda de un controlador Bus Master DMA con control propio. Así se pueden alcanzar velocidades de 8 a 16 Mb. por segundo.

El interface:

IDE:

Cronologicamente, y empezando por el primero nos encontramos con los primeros discos IDE con su limitación a 528 Mb. y pudiendo solo conectar hasta 2 de ellos.

Elementos de Arquitectura y Seguridad Informática

Después vinieron los discos EIDE (FastATA), desarrollados por la compañía Western Digital, compatibles con los primeros, pero con algunas mejoras, basadas en la especificación ATA-2, que ya soporta unidades de CD-ROM (ATAPI) y de cinta.

Otra mejora importante es el soporte de 2 canales para conectar hasta 4 unidades.

Además se definen varios modos de transferencia de datos, que llegan hasta los 16,6 Mb./seg. como el PIO-4, o mejor aún el DMA-2, que soporta la misma tasa pero sin intervención de la CPU.

La última especificación, desarrollada por Quantum es la Ultra DMA/33 (UltraATA), que permite transferencias DMA a 33 Mb./seg.

SCSI:

En el caso de los discos SCSI, tenemos el primero, llamado SCSI-1, con un ancho de bus de 8 bits, aunque ya en esta primera especificación se incluían características muy destacadas, como la posibilidad de conectar hasta 7 dispositivos de todo tipo, discos, cintas, escáners, CD-ROM, etc...

Después viene el SCSI-2, que ya dispone de un ancho de bus de 16 bits. El siguiente paso es el Fast-SCSI, considerado el doble de rápido. Después viene el Wide SCSI, ya con un ancho de bus de hasta 32 bits, así como un mayor rendimiento.

Instalación de varios dispositivos:

En el caso de querer instalar más de un dispositivo IDE, hay que tener en cuenta algunos detalles muy importantes.

En las controladoras EIDE, disponemos de dos canales IDE independientes, con lo que podemos llegar a instalar hasta cuatro dispositivos, dos por canal. El primer dispositivo de cada canal se conoce como "maestro" (maestro) y el segundo como "slave" (esclavo).

En un canal cualquiera, sólo un dispositivo puede hacerse con el control del bus, es decir, no pueden utilizar el bus concurrentemente, con lo que si ponemos dos discos en el mismo canal, estos se "pelearan" por él, y el rendimiento de ambos bajará notablemente.

En el caso de tener sólo dos dispositivos, se deberán poner a ambos como "maestros", uno en cada canal, es decir, conectaremos un cable a cada disco, y cada cable irá a un conector en la placa base. Es aconsejable que el disco más rápido sea colocado en el primer canal (Primario), pues aparte de ser el disco que arranca el sistema operativo, es donde, normalmente, está ubicado el archivo de intercambio de la memoria virtual, con lo que el rendimiento general del equipo aumentará.

Si tenemos dos discos y un CD-ROM, el CD-ROM se colocará como "esclavo" del segundo canal (secundario). Esto es así porque normalmente el segundo disco

tendrá menos actividad que el primero (recordemos que Windows y otros sistemas operativos hacen un uso intensivo del archivo de intercambio).

Para poder configurar el disco como maestro o como esclavo necesitaremos saber la posición exacta de unos puentes o "jumpers" que normalmente todos los discos poseen. Por desgracia, cada fabricante utiliza su propio criterio.

En la mayoría de los casos, disponemos de 3 puentes, serigrafiados como SP, DS y CS, y en este caso, quitaremos todos los puentes para modo esclavo, y colocaremos uno sólo en "DS" para maestro. En otro caso, deberemos consultar el manual si disponemos de él, o fijarnos en la serigrafía, o en todo caso, acudir a la página web del fabricante. En el caso de disponer de una controladora y dispositivos SCSI, ninguna de estas precauciones es necesaria. Pues SCSI soporta hasta 6 dispositivos concurrentemente (o 14 en los modelos más modernos).

En casi todas las placas 486 y en algunas Pentium antiguas, existe un límite de 528 MB. impuesto por la BIOS

Controladoras de Discos Duro

El interface es la conexión entre el mecanismo de la unidad de disco y el bus del sistema. El interface define la forma en que las señales pasan entre el bus del sistema y el disco duro. En el caso del disco, su interface se denomina controladora o tarjeta controladora, y se encarga no sólo de transmitir y transformar la información que parte de y llega al disco, sino también de seleccionar la unidad a la que se quiere acceder, del formato, y de todas las órdenes de bajo nivel en general. La controladora a veces se encuentra dentro de la placa madre.

Se encuentran gobernados por una controladora y un determinado interface que puede ser:

- **ST506:** Es una interface al nivel de dispositivo; el primer interface utilizado en los PC's. Proporciona un valor máximo de transferencia de datos de menos de 1 Mbyte por segundo (625k por segundo con codificación MFM, y 984k por segundo con codificación RLL). Actualmente esta desfasado y ya no hay modelos de disco duro con este tipo de interface.

- **ESDI:** Es un interface a nivel de dispositivo diseñado como un sucesor del ST506 pero con un valor más alto de transferencia de datos (entre 1,25 y 2.5 Mbytes por segundo). Ya ha dejado de utilizarse este interface y es difícil de encontrar.

IDE: Es un interface a nivel de sistema que cumple la norma ANSI de acoplamiento a los AT y que usa una variación sobre el bus de expansión del AT (por eso también llamados discos tipo AT) para conectar una unidad de disco a la CPU, con un valor máximo de transferencia de 4 Mbytes por segundo. En principio, IDE era un término genérico para cualquier interface al nivel de sistema. La especificación inicial de este interface está mal definida. Es más rápida que los antiguos interfaces ST506 y ESDI pero con la desaparición de los ATs este interface desaparecerá para dejar paso al SCSI y el SCSI-2.

Elementos de Arquitectura y Seguridad Informática

Íntimamente relacionado con el IDE, tenemos lo que se conoce como ATA, concepto que define un conjunto de normas que deben cumplir los dispositivos. Años atrás la compañía Western Digital introdujo el standard E-IDE (Enhanced IDE), que mejoraba la tecnología superando el límite de acceso a particiones mayores de 528 Mb. y se definió ATAPI, normas para la implementación de lectores de CD-ROM y unidades de cinta con interfaz IDE. E-IDE se basa en el conjunto de especificaciones ATA-2. Como contrapartida comercial a E-IDE, la empresa Seagate presento el sistema FAST-ATA-2, basado principalmente en las normas ATA-2. En cualquier caso a los discos que sean o bien E-IDE o FAST-ATA, se les sigue aplicando la denominación IDE como referencia.

Para romper la barrera de los 528 Mb. las nuevas unidades IDE proponen varias soluciones:

El **CHS** es una traducción entre los parámetros que la BIOS contiene de cilindros, cabezas y sectores (ligeramente incongruentes) y los incluidos en el software de sólo lectura (Firmware) que incorpora la unidad de disco.

El **LBA** (dirección lógica de bloque), estriba en traducir la información CHS en una dirección de 28 bits manejables por el sistema operativo, para el controlador de dispositivo y para la interfaz de la unidad.

Debido a la dificultad que entraña la implemetación de la compatibilidad LBA en BIOS, muchos de los ordenadores personales de fabricación más reciente continúan ofreciendo únicamente compatibilidad con CHS. El techo de la capacidad que permite las solución CHS se sitúa en los 8,4 Gb, que por el momento parecen suficientes.

SCSI: Es un interface a nivel de sistema, diseñado para aplicaciones de propósito general, que permite que se conecten hasta siete dispositivos a un único controlador. Usa una conexión paralela de 8 bits que consigue un valor máximo de transferencia de 5 Mbytes por segundo. Actualmente se puede oír hablar también de SCSI-2 que no es más que una versión actualizada y mejorada de este interface. Es el interface con más futuro, si bien tiene problemas de compatibilidad entre las diferentes opciones de controladoras, discos duros, impresoras, unidades de CD-ROM y demás dispositivos que usan este interface debido a la falta de un estándar verdaderamente sólido.

Las mejoras del SCSI-2 sobre el SCSI tradicional son el aumento de la velocidad a través del bus, desde 5 Mhz a 10 Mhz, duplicando de esta forma el caudal de datos. Además se aumenta el ancho del bus de 8 a 16 bits, doblando también el flujo de datos. Actualmente se ha logrado el ancho de 32 bits, consiguiendo velocidades teóricas de hasta 40 Mbytes / seg.

Los interfaces IDE y SCSI llevan la electrónica del controlador en el disco, por lo que el controlador realmente no suele ser mas que un adaptador principal para conectar el disco al PC. Como se puede ver unos son interfaces a nivel de dispositivo y otros a nivel de sistema, la diferencia entre ambos es:

INTERFACE A NIVEL DE DISPOSITIVO: Es un interface que usa un controlador externo para conectar discos al PC. Entre otras funciones, el controlador convierte la ristra de datos del disco en datos paralelos para el bus del microprocesador principal del sistema. ST506 y ESDI son interfaces a nivel de dispositivo.

· **INTERFACE A NIVEL DE SISTEMA:** Es una conexión entre el disco duro y su sistema principal que pone funciones de control y separación de datos sobre el propio disco (y no en el controlador externo), SCSI e IDE son interfaces a nivel de sistema.

Estructura lógica de los discos duros

Lo que interrelaciona los discos duros con los disquetes, es su estructura, que se resumen en diferentes funciones del BIOS, que sirven entre otras cosas para el acceso a los mismos.

En primer lugar, internamente los discos duros se pueden dividir en varios volúmenes homogéneos. Dentro de cada volumen se encuentran una estructura que bajo el sistema operativo del Ms-Dos, sería la siguiente:

Sector de Arranque.
Primera tabla de localización de archivos (FAT).
Una o más copias de la FAT.
Directorio Raíz (eventualmente con etiqueta de volumen).
Zona de datos para archivos y subdirectorios.

Como se muestra en el cuadro anterior, cada volumen se divide en diferentes zonas que por una parte acogen las diferentes estructuras de datos del sistema de archivos, y por otra los diferentes archivos y subdirectorios. En dicho cuadro no se han hecho referencia al tamaño de las diferentes estructuras de datos y zonas. Pero no es posible describirlas, ya que se adaptan individualmente al tamaño del volumen correspondiente

· **El Sector de Arranque :** Al formatear un volumen, el sector de arranque se crea siempre como primer sector del volumen, para que sea fácil de localizar por el DOS. En él se encuentra información acerca del tamaño, de la estructura del volumen y sobre todo del BOOTSTRAP-LOADER, mediante el cual se puede arrancar el PC desde el DOS. A ésta parte se le llama sector de arranque (BOOT).

· **La Tabla de Asignación de Ficheros (File Allocation Table) (FAT) :** Si el DOS quiere crear nuevos archivos, o ampliar archivos existentes, ha de saber qué sectores del volumen correspondiente quedan libres, Estas informaciones las toma la llamada FAT. Cada entrada a esta tabla se corresponde con un número determinado de sectores, que son adyacentes lógicamente en el volumen. Cada uno de estos grupos de sectores se llama **Cluster**. El tamaño de las diferentes entradas de esta

Elementos de Arquitectura y Seguridad Informática

tabla en las primeras versiones del DOS era de 12 bits. con lo que se podían gestionar hasta 4.096 Clusters, correspondiente a una capacidad aproximada de 8 Mbytes. En vista del problema que surgió al aparecer discos duros de capacidades más elevadas, se amplió el tamaño a 16 bits., permitiendo el direccionamiento de un máximo de 65.535 Clusters. Actualmente se está creando FAT's de hasta 32 bits, para discos duros capaces de almacenar Gigas de información.

Una o más copias de la FAT : El DOS permite a un programa de formateo crear no sólo una, sino varias copias idénticas de la FAT. Si el DOS encuentra uno de estos medios, cuida todas las copias de la FAT simultáneamente, así que guarda allí los nuevos clusters ocupados o liberados al crear o borrar archivos. Esto ofrece la ventaja de que se puede sustituir la FAT primaria en caso de defecto por una de sus copias, para evitar la pérdida de datos.

· **El directorio Raíz :** La cantidad máxima de entradas en el directorio raíz se limita por su tamaño, que se fija en el sector de arranque. Ya que el directorio raíz representa una estructura de datos estática, que no crece si se guardan más y más archivos o subdirectorios. De ahí que, dependiendo del tamaño, bien un disco duro o bien de volumen, se selecciona el tamaño del directorio raíz en relación al volumen.

· **La Zona de Datos :** Es la parte del disco duro en la que se almacena los datos de un archivo. Esta zona depende en casi su totalidad de las interrelaciones entre las estructuras de datos que forman el sistema de archivos del DOS, y del camino que se lleva desde la FAT hacia los diferentes sectores de un archivo.

Torres Iomega (MO, ZIP, JAZZ)

Tiempo más tarde surgió una unidad de almacenamiento removible, conectable a un puerto SCSI, que utilizaba unos cartuchos parecidos a los disquettes, pero que lograban contener 100 Mb. en datos. Esta unidad es la Zip de Iomega, que con el tiempo se ha ido convirtiendo en una seria alternativa al disquette de 1,44. Hoy en día se ha abaratado su coste, tanto la unidad en sí como los cartuchos, y se han creado unidades conectables al puerto IDE y a la salida paralelo del ordenador, habiendo, por tanto unidades internas y externas. También se ha conseguido que muchos fabricantes de placas base incorporen en sus ROM's código para hacerlas autoarrancables, y así poder substituir por completo a la disquetera tradicional.

Imation LS-120

Más tarde, Imation, actualmente una división de 3M, sacó al mercado una disquetera, capaz de leer y grabar en todos los formatos del estándar de 3 1/2, pero que también permite, con unos disquettes especiales y en un nuevo formato, almacenar 120 Mb.

Esta unidad recibe el nombre de LS-120, y actualmente algunas empresas como Panasonic, ya están comercializando unidades tanto externas, conectables al puerto paralelo, como internas conectables al IDE. Al igual que la ZIP de iomega, también está implementada en la ROM de algunos ordenadores para ser usada como unidad de arranque.

Streamers

Las unidades de cinta o streamers emplean un sistema similar al de casete de audio. Su capacidad puede variar entre 40 Megas y varios Gigas, y son ideales para realizar grandes copias de seguridad (backups), en los que el tiempo no sea importante, ya que su mayor desventaja estriba en su notoria lentitud, tanto al grabar como al recuperar la información; en este último punto hay que tener en cuenta que al ser un sistema secuencial, para localizar un dato debe pasar primero por los que se encuentren almacenados previamente.

También es importante saber que estos dispositivos suelen aportar la característica de compresión, por lo que la capacidad que proclaman en su publicidad es siempre la que se obtiene al comprimir la información. En otras palabras, hay que informarse bien de la capacidad de la unidad con y sin compresión. Y también asegurarse de que las cintas usadas cumplen, al menos, con el estándar QIC; y si también permiten el uso de cintas Travan (otro estándar), mucho mejor.

Cintas DAT

Existe una variante de las cintas streamers normales: las cintas DAT (Digital Audio Tape o Cinta Digital de Audio). Se trata de cintas de cuatro milímetros, bastante más pequeñas que las normales QIC y similares a las empleadas en la industria musical. Su capacidad se mide en gigabytes, normalmente más de dos.

Su velocidad es también bastante mayor que la de las QIC, y su implementación suele hacerse invariablemente con SCSI; por supuesto, también son ideales para grandes copias de seguridad. Y seguro que ya os imagináis la desventaja: el precio. Estas unidades no suelen bajar de los veinte mil duros, lo que unido a sus especiales características las hacen más propias de entornos profesionales (servidores de red, etc.) que de usuarios domésticos.

CD y DVD-ROM

La unidad de CD-ROM ha dejado de ser un accesorio opcional para convertirse en parte integrante de nuestro ordenador, sin la cual no podríamos ni siquiera instalar la mayor parte del software que actualmente existe, por no hablar ya de todos los programas multimedia y juegos.

Pero vayamos a ver las características más importantes de estas unidades.

En primer lugar vamos a diferenciar entre lectores, grabadores y regrabadores. Diremos que los más flexibles son los últimos, ya que permiten trabajar en

Elementos de Arquitectura y Seguridad Informática

cualquiera de los tres modos, pero la velocidad de lectura, que es uno de los parámetros más importantes se resiente mucho, al igual que en los grabadores.

Es uno de los aspectos más importantes es la velocidad. Está claro que cuanto mayor sea la velocidad, mejor será la respuesta del sistema a la hora de leer datos y reproducir sonido y vídeo desde el CD. Los valores que se han ido tomando, son 1x, 2x, 3x, 4x, 6x, 8x, 10x, 12x, 14x, 16x, 18x, 24x, 28x, 32x, 36x, 40x y llegan hasta 52x (es posible que a más). La x hay que sustituirla por 150 Kb/seg.

Dado que las unidades lectoras son bastante económicas, suele ser habitual contar con una lectora, y una regrabadora, usando la segunda sólo para operaciones de grabación.

En cuanto a las velocidades de grabación suelen estar sobre las 2X en regrabadoras y las 2, 4 y hasta 8x en grabadoras).

Y después de la velocidad de lectura y grabación nos encontramos con otro tema importante como es el tipo de bus. Al igual que en los discos, este puede ser SCSI o EIDE. Aconsejamos SCSI (Ultra Wide) para entornos profesionales y EIDE (Ultra DMA) para los demás.

Otro aspecto que vamos a comentar es el tipo de formatos que será capaz de leer / grabar. Es interesante que sea capaz de cumplir con todos:

- ISO 9660: Imprescindible. La mayor parte de los demás son modificadores de este formato.
- CD-XA y CD-XA entrelazado: CD's con mezcla de música y datos.
- CD Audio: Para escuchar los clásico Compact Disc de música.
- CD-i: Poco utilizado.
- Vídeo-CD: Para películas en dicho formato.
- Photo-CD Multisesión: Cuando llevas a revelar un carrete puedes decir que te lo graben en este formato.

Velocidad de acceso

Es el tiempo medio que tarda la unidad en acceder a los datos cuando se los pedimos. Los valores típicos oscilan entre 100-250 ms. Está claro que cuanto menor sea el valor, mejor.

Tamaño del buffer

El buffer es una memoria especial que se encarga de transferir la información del CD al interfaz. No se trata de una memoria caché, pero permite enviar datos en paquetes más grandes, con lo que se logran mayores transferencias (pero no milagrosas). Los valores típicos van desde los 64 a los 512 Kb.

Compatibilidad

CD-XA, CD-1 (M2, F2), PhotoCD, multisesión, CD grabable y regrabable, son distintos tipos de CD-ROM que se pueden leer en una unidad que especifique qué es compatible con estos sistemas. Por ejemplo CD-XA quiere decir arquitectura avanzada; CD-I puede leer CD-I de Phillips y Video CD. PhotoCD lee el formato multisesión de discos de fotografías Kodak. Hay algunas unidades que permiten leer discos Macintosh para poder utilizarlas en este tipo de unidades.

Dispositivos de disco compacto

Tratando un poco más el disco compacto como tal podemos plantear que, de forma similar a un disco duro o un disquete la información en un CD se organiza concéntricamente en un disco que rota a determinadas velocidades alrededor de un punto central. La velocidad del CD no es constante sino que se incrementa el número de revoluciones por minuto (rpm) para las pistas más cercanas a la periferia, lo cual hace que se mantenga la misma cantidad de datos pasando frente al cabezal en cada momento. La distancia a cubrir para una cantidad de datos es siempre mayor en el borde que en el interior, este proceso se conoce como CLV (Constant Linear Velocity.) Los CD ROM giran con velocidades usuales entre 215 y 625 rpm.

Las unidades para almacenar información son codificadas como pequeñas depresiones sobre un cristal (.capa sintética transparente) especialmente pulido y limpio mediante ultrasonido, se realiza la grabación de los "pits" (fig. 1) mediante la energía de un rayo láser azul. Estas pequeñas incisiones que produce el rayo láser al cortar la capa sintética son las que darán origen a la señal digital.

La capa de aluminio cuenta con depresiones (pit) y no depresiones (land) (Figura IV.2) distribuidas por su superficie. Cada transición de land a pit ó de pit a land se interpreta como un uno lógico y cada no-transición como un cero lógico. Las posiciones de un pit o un land tienen un ancho de 0.5 micra de milímetro ($1\mu\text{m}=0.001\text{ mm}$) y se espacian 1 micra de milímetro aproximadamente uno del otro. Sin tocar la superficie un rayo láser rastrea los pits y la electrónica los convierte en bytes y cadenas coherentes de información.

Dado que las pistas son tan estrechas no es posible detectar los bits individualmente, razón por la que se expande el método pit-land al denominado modulación EFM (Eighth to Fourteen) que establece la condición de que cada dos valores de cero en el siguiente o al menos después de once valores aparezca un uno a continuación. Por no ser suficiente para este caso el método tradicional de codificación en bytes (8 bits) se pasa a los 14 bits, existiendo una tabla de conversión que asigna un número de 14 bits a cada valor de 8 bits.

COMPARATIVA DE DIMENSIONES

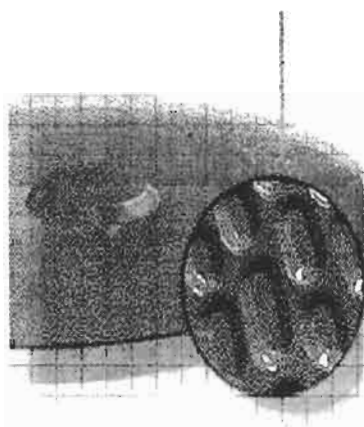


Figura IV.2. Esquema que muestra la superficie ampliada de un CD

A continuación se describe a grandes rasgos el proceso de fabricación y duplicado de los CD en las fábricas:

Sobre un cristal especialmente pulido y limpio mediante ultrasonidos, y recubierto por una fina capa de laca, se realiza la grabación de los pits mediante la energía de un rayo láser azul. Estas pequeñas inscripciones que produce el rayo láser al cotar la laca son las que darán origen a la señal digital. Para hacer conductivo el cristal grabado, y por tanto útil para la electrólisis o galvanizado, se le recubre de una fina capa de plata al 99.999% de pureza. Para ello, se introducen varios hilos de plata en una campana de vacío y se calientan hasta que se funden (temp. fusión de la plata 1200 °C) y vaporizan, por lo que las partículas se depositan sobre la cara grabada del cristal.

EL DVD: ¿un nuevo estándar?

La especificación DVD -según algunos fabricantes, Digital Vídeo Disc, según otros, Digital Versatile Disc-, no es más que un nuevo intento por unificar todos los estándares óptico-digitales de almacenamiento, es decir, cualquier sistema de grabación que almacene imágenes o sonido. DVD abarca todos los campos actualmente existentes, por lo que, si llega a implantarse, un mismo disco DVD podrá utilizarse para almacenar películas, música, datos informáticos, e incluso los juegos de consolas.

Las siglas DVD se traducen como Digital Video Device (dispositivo de vídeo digital) o bien Digital Versatile Disc (disco digital versátil). Resulta curiosa esta duplicidad de interpretaciones, que nos hace advertir que mientras unos lo consideran un

simple almacenaje para vídeo, otros prefieren destacar que tiene muchas otras aplicaciones.

A primera vista, un disco DVD es prácticamente indistinguible de un CD convencional; quizá tiene un brillo más o menos particular, pero dejando aparte esto nos encontramos con la clásica oblea redonda de material plástico, de 12 cm de diámetro y con el agujero en el centro. Entonces, ¿qué le diferencia del clásico CD-ROM o del aún más clásico CD de música?

La gran ventaja del DVD, con relación a los sistemas actuales, es su mayor velocidad de lectura -hasta 4 veces más que los reproductores CD tradicionales-, y su gran capacidad de almacenamiento, que varía entre los 4.7 y los 17 Gigas, es decir, el tamaño aproximado de 25 CD-ROM. Todo ello, en un disco DVD que, externamente, es exactamente igual que un CD tradicional. Esta elevada capacidad permite, no sólo almacenar gran cantidad de información, aplicable a todo tipo de enciclopedias, programas o bases de datos, sino también reproducir 133 minutos de vídeo con calidad de estudio, sonido Dolby Surround AC-3 5.1, y 8 pistas multilenguaje para reproducir el sonido en 8 idiomas, con subtítulos en 32 idiomas. Estos minutos pueden convertirse en varias horas, si se disminuye la calidad de la imagen hasta los límites actuales. Las más importantes compañías electrónicas, los más influyentes fabricantes de hardware y software, y las más sobresalientes compañías cinematográficas y musicales están apoyando fuertemente el proyecto.

No obstante, pese a todas estas características tan espectaculares, la gran baza de la tecnología DVD está todavía por desvelar: gracias a la compatibilidad con los sistemas actuales, los lectores DVD-ROM son capaces de leer los CD-ROM y CD musicales que actualmente existen, por lo que el cambio de sistema será mucho más llevadero, ya que podremos seguir utilizando los cientos de millones de discos digitales existentes en el mercado.

Mientras que de nuestro viejo amigo el CD sólo existía un tipo (aparte de los mini-CDs de 8 cm), en el DVD tenemos hasta **4 variedades** (y esto sin contar los grabables): una cara y una capa, una cara y dos capas, dos caras y una capa y dos caras y dos capas. Cara se refiere a las dos del disco DVD: la de adelante y la de detrás (de nuevo una solución simple pero eficaz); capa es algo más complicado, se refiere a capas de material (y por tanto de información) superpuestas en la misma cara del disco.

Así, la **capacidad** de un DVD va desde los **4,7 GB** de la variedad de una cara y una capa hasta los **17 GB** de la de dos caras y dos capas; o, equivalentemente, la capacidad **de 7 a 26 CDs** convencionales..

Para ver la diferencia necesitaríamos un microscopio; en el DVD, al igual que en el CD, la información digital se representa mediante microscópicas marcas como agujeritos en la superficie del CD (tapadas por una resina transparente protectora). Lo que ocurre es que en el DVD dichas marcas son más pequeñas y están más juntas, por lo que al haber más la capacidad es mayor (Figura IV.3) . ¿Simple, verdad?

Elementos de Arquitectura y Seguridad Informática

¿Y para qué sirve tanta capacidad, se preguntará usted? . Para distribuir programas no, sin duda, porque ¿Se imagina que la nueva versión de Word ocupara más de los 650 MB de un CD-ROM? No, la principal función es el almacenaje de vídeo digital, para lo cual 17 GB no es una cifra demasiado exagerada como la variedad más común de DVD es la de una cara y una capa, resultan algo más de 2 horas de vídeo; suficiente para una película con mayor calidad que en VHS, doblada en varios idiomas y con subtítulos en algunos más, a elección del usuario.

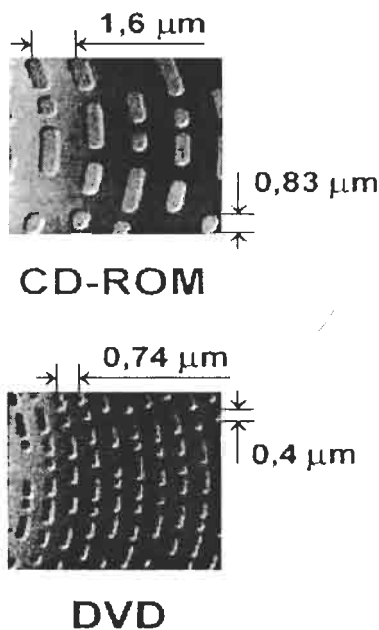


Figura IV.3. Muestra comparativa de la superficie de un CD y DVD.

En el formato **MPEG-2**, un formato de compresión de vídeo digital (en el que emiten Canal Satélite y Vía Digital, por ejemplo), esos 17 GB se quedan en menos de 10 horas (eso sí, con sonido Dolby Digital AC-3). Y ¿Escalofriante, verdad? Esta elevada capacidad permite, no sólo almacenar gran cantidad de información, aplicable a todo tipo de enciclopedias, programas o bases de datos, sino también reproducir 133 minutos de vídeo con calidad de estudio, sonido Dolby Surround AC-3 5.1, y 8 pistas multilinguaje para reproducir el sonido en 8 idiomas, con subtítulos en 32 idiomas. Estos minutos pueden convertirse en varias horas, si se disminuye la calidad de la imagen hasta los límites actuales.

Los DVD para datos informáticos se denominan DVD-ROM, mientras que los de vídeo se denominan DVD-Vídeo o simplemente DVD. También existen normas que

definen DVDs de 8 cm, pero probablemente se usen tan poco como los CDs de ese tamaño.

La especificación DVD-ROM

Pese a que los lectores DVD-Vídeo y DVD-Audio son, a priori, muy interesantes, vamos a centrarnos en los lectores DVD-ROM. Pero, antes de discutir sus posibilidades, vamos a conocer todas sus características principales.

Los lectores DVD-ROM más básicos nos permiten leer discos DVD-ROM - obviamente, así como CD musicales y CD-ROM, a una velocidad 8X, es decir, 1200 Ks/sg, y un tiempo de acceso situado entre los 150 y 200 milisegundos. Esta compatibilidad es posible, no sólo porque soporta el estándar ISO 9660 utilizado por los CD-ROM, sino también porque los discos, externamente, son iguales a los CD convencionales. Al contrario que los CD-ROM, existen discos DVD de distinto tamaño. Todos están formados por dos capas de sustratos de 0.6 mm, que se unen para formar un sólo disco.

En primer lugar, tenemos los discos que podemos considerar estándar (120 mm), de una cara, una capa, y una capacidad de 4.7 Gigas, o 133 minutos de vídeo de alta calidad, reproducido a una velocidad de 3.5 Megas. Puesto que un CD-ROM sólo puede almacenar 650 Megas, este espacio es el equivalente a 6 CD-ROM. Estos serán los discos utilizados para almacenar películas.

Llegados este punto, hay que decir que los Gigas ofrecidos por los fabricantes de unidades DVD, no se corresponden exactamente con Gigas informáticos, ya que los primeros utilizan múltiplos de 1000, mientras que en informática, el cambio de unidad se realiza multiplicando o dividiendo por 1024. Así, los 4.7 Gigas de esta primera clase de discos se corresponden con 4.38 Gigas informáticos, mientras que 17 Gigas equivalen a 15.9 Gigas reales. A pesar de ello, mantendremos durante todo el artículo la primera nomenclatura, ya que es la utilizada por los diferentes fabricantes.

Continuaremos con el segundo tipo de disco DVD. Hasta ahora, hemos hablado de los discos de una cara, y una capa. Si se almacena información en la segunda cara, entonces tenemos un disco de dos caras y una capa, con 9.4 Gigas de capacidad. También es posible añadir una segunda capa a cualquiera de las dos caras. Esta doble capa utiliza un método distinto al de los CD tradicionales, ya que se implementa mediante resinas y distintos materiales receptivos/reflectantes. Si la capa es de 120 mm, y dispone de una sola cara, la cantidad almacenada es de 8.5 Gigas, o 17 Gigas si dispone de dos caras. En el caso, también posible, de que la capa disponga de un grosor de 80 mm, la capacidad se sitúa entre los 2.6 y 5.3 Gigas de capacidad -simple o doble cara-. Puede parecer un galimatías, pero sólo se trata de distintos discos con distintas capacidades

Para leer la información, el lector DVD-ROM utiliza un láser rojo con una longitud de onda situada entre los 630 y los 650 nanómetros, frente a los 780 nanómetros de los CD convencionales. Otras diferencias, con respecto a la arquitectura de los CD-

Elementos de Arquitectura y Seguridad Informática

ROM, está en el tamaño de las pistas y los pits -marcas que guardan la información-, ya que son más pequeños, por lo que hay muchos más y, consecuentemente, se almacena más información.

Con estos primeros datos, podemos sacar las primeras conclusiones. En primer lugar sobresalen, por encima de todo, sus grandes ventajas: la compatibilidad CD y CD-ROM, su velocidad, y la gran capacidad de almacenamiento, que varía entre los 1.4 y los 17 Gigas. Todas las aplicaciones que, por definición, necesiten una gran cantidad de espacio, se verán beneficiadas: bases de datos, programas con secuencias de vídeo, recopilaciones, enciclopedias, etc. Estas últimas podrán mejorar su contenido, al añadir muchos más vídeos, animaciones y sonidos. Igualmente, se podrán comercializar las versiones dobladas de un programa en todos los idiomas, y en un sólo disco. A pesar de todo, como cualquier tecnología nueva, no está exenta de problemas. El primero de ellos es la incompatibilidad con ciertos estándares. En algunos casos, como puede ser el laserdisc, es inevitable, ya que se trata de discos de diferentes tamaños.

Pero, a estas alturas, todavía no está muy claro si las unidades DVD serán compatibles Photo CD y CD-I. Los DVD-ROM tampoco pueden leer CD-R, es decir, CD-ROM grabados con una grabadora de CD-ROM. De forma recíproca, una grabadora CD-R no puede crear discos DVD.

La compatibilidad CD-R es un tema tan importante que es posible que quede solucionado en muy poco tiempo, incluso antes de que los lectores DVD-ROM vean la luz en el mercado europeo.

Un CD-ROM grabado no es reconocido por un lector DVD-ROM, debido a que utiliza un láser con una longitud de onda que es incapaz de detectar las marcas realizadas en un CD-R. Esta limitación tecnológica provocaría que millones de CD-R grabados con valiosa información quedasen inutilizados, por lo que ya se han propuesto distintas medidas para superarlo. En primer lugar, los fabricantes de CD-ROM grabables están trabajando en un nuevo formato de disco llamado CD-R 2, que permitirá a las grabadoras actuales crear CD-R que pueden ser leídos en las unidades DVD-ROM. Para reconocer los discos ya grabados en el formato CD-R 1, se barajan distintas soluciones. Samsung ha anunciado que sus lectores DVD dispondrán de unas lentes holográficas que reconocerán los CD-R. Los reproductores de Sony irán equipados con dos lasers, uno para leer DVD-ROM, y otro para los CD y CD-R. Philips también asegura su compatibilidad con los discos grabados... En definitiva, parece ser que este tema quedará solucionado a lo largo del año.

Otra de las dificultades tiene que ver con la reproducción de películas en el ordenador. El estándar utilizado por el sistema DVD-Vídeo es el formato MPEG-2, a una velocidad de 24 fps (cuadros por segundo). El problema es que ni siquiera los ordenadores más potentes son capaces de soportar semejante flujo de datos por segundo.

En la actualidad, los ordenadores equipados con la tarjeta apropiada (adquirida en el último año) pueden reproducir vídeo MPEG-1, que dispone de una calidad inferior al mencionado formato MPEG-2. Para solucionar esto, existen distintos enfoques, tal como se explica en uno de los recuadros adjuntos.

Todo se reduce a comercializar tarjetas gráficas compatibles MPEG-2, o incluir los chips necesarios en los propios lectores de DVD-ROM.

Como podemos observar, los posibles obstáculos van a poder ser solucionados en muy poco tiempo, por lo que las posibilidades que se nos avecinan no pueden ser más prometedoras, posibilidades que se verán reflejadas en las actuales unidades que están a punto de ser comercializadas.

Algunas cuestiones importantes sobre el DVD

Llegados a este punto en que usted ya sabe lo que es el DVD (una especie de CD apretado que se usa sobre todo para guardar vídeo), vamos a lo práctico, en forma de preguntas típicas y respuestas:

¿Puedo usar un disco DVD en mi unidad de CD-ROM normal? **No**, para nada; necesita de una unidad lectora de DVDs, que cuestan como el doble de una de CD-ROM de marca.

¿Puedo usar mis CDs en una unidad de DVD? **Depende**. Los CDs de audio y los CD-ROMs normales, sí, sin problemas. Los CDs grabables (como las copias habituales de CDs), depende de la unidad pero es probable que sí. Los CDs regrabables, probablemente no, pero algunos lectores de DVD son capaces de hacerlo.

¿Cómo son de rápidas estas unidades de DVD? Las hay fundamentalmente de velocidad "1x" y de "2x". Las **1x** están totalmente desfasadas, aunque llegan como mínimo a 1,2 MB/s (el equivalente a un CD de 8x). Las de **2x** llegan como poco hasta 2,4 MB/s, el equivalente a un CD 16x, y a veces 20x o incluso más si en vez de un DVD hemos introducido un CD-ROM.

¿Necesito algo más para ver el vídeo digital? **Sí**. Necesita una tarjeta descompresora de vídeo MPEG-2, que a veces viene con la unidad DVD y a veces no. Además, deberá tener un ordenador potente, digamos un Pentium 133 con 32 MB de RAM.

¿Existen unidades de DVD grabables? **Sí, pero no estándar**. Existen al menos dos tipos distintos e incompatibles.

Conclusiones

Es que **al DVD le falta algo para sustituir al VHS: grabar**. Si se pudiera grabar, podría sustituir al CD-ROM, al vídeo VHS y al CD y la casete del equipo de música.

Sin embargo, para los usos de distribución, basta con la capacidad de un CD o dos; como unidad para copias de seguridad necesitamos grabar, pero aún tienen problemas al leer CDs grabables y regrabables; y las unidades grabables se

Elementos de Arquitectura y Seguridad Informática

encuentran en un peligroso estado embrionario. Por cierto: los discos DVD son aún más delicados frente al polvo y las huellas dactilares que los CD-ROM.

V. Tarjetas de expansión e interfaces

Conectores: PCI, AGP...

La tarjeta gráfica, como añadido que es al PC, se conecta a éste mediante un slot o ranura de expansión. Muchos tipos de ranuras de expansión se han creado precisamente para satisfacer a la ingente cantidad de información que se transmite cada segundo a la tarjeta gráfica.

ISA: el conector original del PC, poco apropiado para uso gráfico; en cuanto llegamos a tarjetas con un cierto grado de aceleración resulta insuficiente. Usado hasta las primeras VGA "**aceleradoras gráficas**", aquellas que no sólo representan la información sino que aceleran la velocidad del sistema al liberar al microprocesador de parte de la tarea gráfica mediante diversas optimizaciones.

VESA Local Bus: más que un slot un bus, un conector íntimamente unido al microprocesador, lo que aumenta la velocidad de transmisión de datos. Una solución barata usada en muchas placas 486, de buen rendimiento pero tecnológicamente no muy avanzada.

PCI: el estándar para conexión de tarjetas gráficas (y otros múltiples periféricos). Suficientemente veloz para las tarjetas actuales, si bien algo estrecho para las 3D que se avecinan.

AGP: tampoco un slot, sino un puerto (algo así como un bus local), pensado únicamente para tarjetas gráficas que transmitan cientos de MB/s de información, típicamente las 3D. Actualmente tiene poca o nula ganancia frente a PCI, pero más futuro como conector dedicado exclusivamente a estos fines.

En cualquier caso, el conector sólo puede limitar la velocidad de una tarjeta, no la eleva, lo que explica que muchas tarjetas PCI sean muchísimos más rápidas que otras AGP más baratas o peor fabricadas.

El AGP: realidades y ficción

Las siglas AGP corresponden a Advanced Graphics Port, o Puerto Avanzado de Gráficos. Se trata de un nuevo sistema para conectar periféricos en la placa base del PC; es decir, es un nuevo bus por el que van datos del microprocesador al periférico. Su propio nombre nos define este nuevo bus: **Puerto**, puesto que se comunica con el micro de manera más íntima que otros buses como PCI (a costa de permitir sólo 1 slot); **Avanzado**, como corresponde a una tecnología moderna que pretende superar las limitaciones del PCI; y **de Gráficos**, ya que ha sido diseñado pensando en ese uso exclusivamente.

El objetivo a la hora de crear este bus era conseguir una tasa de transferencia de datos micro-tarjeta gráfica superior a la que ofrece el PCI de 32 bits a 33 MHz, 132 MB/s. Esta tasa resulta suficiente para aplicaciones 2D, pero insuficiente (al menos en teoría) para las nuevas tarjetas 3D, que deben transmitir varios "megas" de

Elementos de Arquitectura y Seguridad Informática

texturas para obtener el máximo realismo. En la actualidad, las placas para Pentium II con el chipset LX ofrecen AGP, mientras que en el mercado de placas socket 7 (para Pentium MMX, AMD K6...) ya existen algunas placas que lo soportan, pero no con chipsets Intel (como el TX), a quien no le interesa favorecer este mercado.

Tipos de AGP: Como muchas tecnologías jóvenes, AGP fue lanzado al mercado en cuanto estuvo preparado, aunque aún no se hubiera afinado del todo. Por ello, existen varios modos de AGP:

AGP 1x: modo con bus de 32 bits y a 66 MHz. Su tasa teórica de transferencia máxima es de **264 MB/s**. En la actualidad, pocas tarjetas de marca tienen sólo este modo.

AGP 2x: modo con bus de 32 bits y a 66 MHz reales, o 133 MHz "virtuales" gracias a la comunicación bidireccional simultánea (parecido al full duplex de las tarjetas de sonido). Su tasa teórica de transferencia máxima es de **528 MB/s**. Es el actualmente usado por las tarjetas de calidad.

AGP 4x: nuevo modo que se implantará en un futuro; tal vez de 800 MB/s (32 bits a 100 MHz).

Sin duda alguna, el modo 1x es un modo "experimental", sacado al mercado con prisas. Su rendimiento es y será indistinguible del de PCI, así que su tiempo de vida a terminado ya (excepto como modo para compatibilidad con tarjetas más antiguas). El modo 2x es el auténtico AGP, aunque como veremos tampoco es la panacea...

¿AGP o PCI?

Los 528 MB/s del AGP 2x (el 1x ni comentarlo) son teóricos. La cuestión es que el chip tiene que repartir su acceso a la memoria con el canal AGP, y con las memorias actuales resulta imposible que se alcance esa cifra de 528 MB/s. Incluso con las modernas SDRAM (las EDO son casi historia), el ancho de bus de memoria es exactamente 528 MB/s, con lo que resulta evidente que si se le da todo al AGP, el micro se queda sin leer la memoria, lo que no puede pasar pues el ordenador no funcionaría, claro.

Así que el rendimiento del AGP 2x baja hasta menos de la mitad, con lo que la diferencia con el PCI se vuelve muy escasa, hasta el punto de que **actualmente casi todas las tarjetas del mercado no ofrecen diferencia con bus AGP o PCI**, o bien diferencias del orden de un 2%. Además, **ni Windows 95 ni NT aprovechan** algunas características importantes del AGP.

Conclusión: el AGP **será un avance** en el momento en que ocurra alguna (a ser posible varias) de estas cuestiones: que las memorias RAM sean aún más rápidas (permitiendo un bus de memoria a 100 MHz de 800 MB/s), que el AGP supere el 2x (probablemente con 100 ó más MHz) o que Windows 98 y NT 5 aparezcan con mejoras en el soporte software.

Que es... la tarjeta de vídeo?

De manera resumida, es lo que transmite al monitor la información gráfica que debe presentar en la pantalla. Con algo más de detalle, realiza dos operaciones:

Interpreta los datos que le llegan del procesador, ordenándolos y calculando para poder presentarlos en la pantalla en forma de un rectángulo más o menos grande compuesto de puntos individuales de diferentes colores (pixels).

Coge la salida de datos digitales resultante de ese proceso y la transforma en una señal analógica que pueda entender el monitor.

Estos dos procesos suelen ser realizados por uno o más chips: el microprocesador gráfico (el cerebro de la tarjeta gráfica) y el conversor analógico-digital o RAMDAC, aunque en ocasiones existen chips accesorios para otras funciones o bien se realizan todas por un único chip.

El microprocesador puede ser muy potente y avanzado, tanto o más que el propio micro del ordenador; por eso algunos tienen hasta nombre propio: Virge, Rage Pro, Voodoo... Incluso los hay con arquitecturas de 128 bits, muchos más que el Pentium.

Pequeña historia de las tarjetas de vídeo

En el principio, los ordenadores eran ciegos; todas las entradas y salidas de datos se realizaban mediante tarjetas de datos perforadas, o mediante el teclado y primitivas impresoras. Un buen día, alguien pensó que era mucho más cómodo acoplar una especie de televisor al ordenador para observar la evolución del proceso y los datos, y surgieron los monitores, que debían recibir su información de cierto hardware especializado: la tarjeta de vídeo.

MDA: En los primeros ordenadores, los gráficos brillaban... por su ausencia. Las primeras tarjetas de vídeo presentaban sólo **texto monocromo**, generalmente en un agradable tono ámbar o verde fosforito que dejaba los ojos hechos polvo en cuestión de minutos. De ahí que se las denominase MDA, Monochrome Display Adapter.

CGA: Luego, con la llegada de los primeros PCs, surgió una tarjeta de vídeo capaz de presentar gráficos: la CGA (Computer Graphics Array, dispositivo gráfico para ordenadores). Tan apasionante invento era capaz de presentar gráficos de varias maneras:

Tabla V-1

CGA	
Resolución (horizontal x vertical)	Colores
320x200	4
640x200	2 (monocromo)

Lo cual, aunque parezca increíble, resultó toda una revolución. Aparecieron multitud de juegos que aprovechaban al máximo tan exiguas posibilidades, además de programas más serios, y los gráficos se instalaron para siempre en el PC.

Elementos de Arquitectura y Seguridad Informática

Hércules: Se trataba ésta de una tarjeta gráfica de corte profundamente profesional. Su ventaja, poder trabajar con gráficos a 720x348 puntos de resolución, algo alucinante para la época; su desventaja, que no ofrecía color. Es por esta carencia por la que no se extendió más, porque jugar sin color no es lo mismo, y el mundo PC avanza de la mano de los diseñadores de juegos (y va muy en serio).

EGA: Otro inventito exitoso de IBM. Una tarjeta capaz de:

Tabla V-2

EGA	
Resolución (horizontal x vertical)	Colores
320x200	16
640x200	16
640x350	16

Estas cifras hacían ya posible que los entornos gráficos se extendieran al mundo PC (los Apple llevaban años con ello), y aparecieron el GEM, el Windows y otros muchos. Sobre las posibilidades de las pantallas EGA, una curiosidad: los drivers EGA de Windows 3.1 funcionan sobre Windows 95, y resulta curioso (y sumamente incómodo, la verdad) ver dicha combinación...

VGA: El estándar, la pantalla de uso obligado desde hace ya 10 años. Tiene multitud de modos de vídeo posibles, aunque el más común es el de 640x480 puntos con 256 colores, conocido generalmente como "VGA estándar" o "resolución VGA".

SVGA, XGA y superiores: El éxito del VGA llevó a numerosas empresas a crear sus propias ampliaciones del mismo, siempre centrándose en aumentar la resolución y/o el número de colores disponibles. Entre ellos estaban:

Tabla V-3

Modo de vídeo	Máxima resolución y máximo número de colores
SVGA	800x600 y 256 colores
XGA	1024x768 y 65.536 colores
IBM 8514/A	1024x768 y 256 colores (no admite 800x600)

De cualquier manera, la frontera entre unos estándares y otros es sumamente confusa, puesto que la mayoría de las tarjetas son compatibles con más de un estándar, o con algunos de sus modos. Además, algunas tarjetas ofrecen modos adicionales al añadir más memoria de vídeo.

La resolución y el número de colores

En el contexto que nos ocupa, la **resolución** es el número de puntos que es capaz de presentar por pantalla una tarjeta de vídeo, tanto en horizontal como en vertical. Así, "800x600" significa que la imagen está formada por 600 rectas horizontales de 800 puntos cada una. Para que nos hagamos una idea, un televisor (de cualquier tamaño) tiene una resolución equivalente de 800x625 puntos.

En cuanto al número de **colores**, resulta casi evidente: los que puede presentar a la vez por pantalla la tarjeta. Así, aunque las tarjetas EGA sólo representan a la vez 16 colores, los eligen de una paleta (sí, como las de pintor) de 64 colores.

La combinación de estos dos parámetros se denomina modo de vídeo; están estrechamente relacionados: **a mayor resolución, menor número de colores representables**, y a la inversa. En tarjetas modernas (SVGA y superiores), lo que las liga es la cantidad de memoria de vídeo (la que está presente en la tarjeta, no la memoria general o RAM). Algunas combinaciones posibles son: (ver tabla IV.5)

Se han colocado los modos más comunes, ya que no todas las tarjetas admiten todos los modos, aparte de que muchas no permiten ampliar la memoria de vídeo. Para los curiosos, el cálculo de la memoria necesaria es: (Res. Vert.)x(Res. Horiz.)x(Bits de color)/8.

Cabe destacar que **el modo de vídeo elegido debe ser soportado por el monitor, ya que si no éste podría dañarse gravemente** (muy gravemente). Esto depende de las características del mismo; en concreto de la Frecuencia Horizontal

La velocidad de refrescamiento

El refrescamiento es el número de veces que se dibuja la pantalla por segundo (como los fotogramas del cine); evidentemente, cuanto mayor sea menos se nos cansará la vista y trabajaremos más cómodos y con menos problemas visuales.

Se mide en hertzios (Hz, 1/segundo), así que 70 Hz significa que la pantalla se dibuja cada 1/70 de segundo, o 70 veces por segundo. Para trabajar cómodamente necesitaremos esos 70 Hz. Para trabajar ergonómicamente, con el mínimo de fatiga visual, 80 Hz o más. El **mínimo absoluto son 60 Hz**; por debajo de esta cifra los ojos sufren muchísimo, y unos minutos bastan para empezar a sentir escozor o incluso un pequeño dolor de cabeza.

Antiguamente se usaba una técnica horrible denominada entrelazado, que consiste en que la pantalla se dibuja en dos pasadas, primero las líneas impares y luego las pares, por lo que 70 Hz entrelazados equivale a poco más de 35 sin entrelazar, lo que cansa la vista sobremedida. Afortunadamente la técnica está en desuso, pero en los monitores de 14" se ha usado hasta hace menos de un par de años.

Tabla V-4

Memoria de vídeo	Máxima resolución (en 2D)	Máximo número de colores
512 Kb	1024x768 a 16 colores	256 a 640x480 puntos
1 MB	1280x1024 a 16 colores	16,7 millones a 640x480
2 MB	1600x1200 a 256 colores	16,7 millones a 800x600
4 MB	1600x1200 a 65.536 colores	16,7 millones a 1024x768

El motivo de tanto entrelazado y no entrelazado es que construir monitores que soporten buenas velocidades de refresco a alta resolución es bastante caro, por lo que la tarjeta de vídeo empleaba estos truquitos para ahorrar a costa de la vista del usuario. Sin embargo, tampoco todas las tarjetas de vídeo pueden ofrecer cualquier velocidad de refresco. Esto **depende de dos parámetros**:

La velocidad del RAMDAC, el convertor analógico digital. Se mide en MHz, y debe ser lo mayor posible, preferiblemente entorno a 175 ó 200 MHz.

velocidad de la memoria de vídeo, preferiblemente de algún tipo avanzado como WRAM o SGRAM.

Memoria de vídeo

Como hemos dicho, su **tamaño** influye en los posibles modos de vídeo (cuanta más, mejor); además, su **tipo** determina si conseguiremos buenas velocidades de refresco de pantalla o no. Los tipos más comunes son:

DRAM: en las tarjetas más antiguas, ya descatalogadas. Malas características; refrescos máximos entorno a 60 Hz.

EDO: o "EDO DRAM". El estándar en tarjetas de calidad media. Muy variables refrescos dependiendo de la velocidad de la EDO, entre 40 Hz (la velocidad de la memoria, no el refresco asociado) las peores y 25 Hz las mejores.

VRAM, WRAM: bastante buenas, aunque en desuso; en tarjetas de calidad, muy buenas características.

MDRAM, SDRAM: dos tipos no muy comunes, pero de alta calidad.

SGRAM: la SDRAM adaptada para uso gráfico. De lo mejor del mercado, va camino de ser estándar.

Adecuación al uso del ordenador

Evidentemente, no es lo mismo elegir una tarjeta gráfica para trabajar en Word en un monitor de 15" que para hacer CAD en uno de 21". Nótese que siempre hago

referencia al monitor con el que van a trabajar, porque una tarjeta muy buena no puede demostrarlo en un mal monitor, ni a la inversa.

Las indicaciones son genéricas en **Ofimática**: tarjetas en formato PCI o AGP, con microprocesadores buenos en 2D, sin necesidades 3D específicas; capaces de 800x600 puntos o 1024x768; con unos 2 MB; y con buenos refrescos, entorno a 70 u 80 Hz. Un ejemplo típico "de marca" es la Matrox Millenium, o cualquiera buena con un S3 Virge.

Juegos y CAD en 3D: con micros especiales para 3D, con mucha memoria (entre 4 y 16 MB), generalmente de marca y preferiblemente AGP. Por ejemplo, para juegos la 3D Blaster de Creative con el chip Voodoo2.

Imágenes y CAD en 2D: con chips de 64 ó 128 bits, memorias ultrarrápidas, capaces de llegar a 1600x1200 puntos a 70 Hz o más, con 2 ó 4 MB. Cualquiera con un superchip, SGRAM y un RAMDAC de 200 MHz o más.

En general, actualmente el tema radica en saber si se necesita o no soporte 3D; la aceleración 2D, es decir, la de Windows, Ofimática, Internet, etc, hace mucho que está más que conseguida; casi todas las tarjetas dan cifras espectaculares y casi indistinguibles en cualquier test 2D.

Cómo cambiar la resolución de pantalla

Primero, deberemos estar seguros de que podemos cambiarla; las tarjetas de vídeo antiguas, como las CGA, EGA o VGA estándar poseen una resolución fija e invariable; las más modernas (SVGA, XGA...) sí pueden variarla entre un abanico más o menos amplio de combinaciones, que dependerán asimismo del número de colores y de la memoria de la tarjeta.

Además, no podemos olvidar que la resolución elegida tendrá que proyectarse en el monitor, por lo que de nada nos sirve una tarjeta capaz de dar 1.024x768 puntos, si el monitor no puede soportar más de 640x480; es más, si sobrepasamos sus capacidades, podemos averiarlo gravemente; por ello, lo primero es una verificación exhaustiva de los manuales de la tarjeta y, especialmente, del monitor.

De cualquier forma, admitir una resolución de 800x600 puntos (también conocida como "SVGA") es casi obligado para cualquier monitor con menos de dos o tres años de edad.

Una vez verificados estos extremos, la forma de cambiar la resolución depende enteramente del sistema operativo en el que trabajemos.

Tarjeta de red

¿Para que sirve una red local? Básicamente para compartir información y recursos, tanto hardware como software. Como ejemplos más concretos podemos citar el poder imprimir en una impresora que está conectada a otro ordenador o directamente a la red como si fuera nuestra propia impresora, o conectarnos a

Elementos de Arquitectura y Seguridad Informática

internet a través de un router mediante una línea RDSI sin necesidad de tener en ninguna estación de trabajo, ni modem, ni línea telefónica, para compartir información a través del correo electrónico, o compartir una base de datos en modo multiusuario, de tal manera que varios usuarios puedan estar modificándola al mismo tiempo.

También conocida como **NIC** (del inglés Network Interface Card), es el elemento que conectaremos al PC para proporcionar el soporte de red. (Figura V.1) Suele venir en formato ISA o PCI; para el Ethernet estándar resulta más que suficiente el ancho de banda de ISA, pero para Fast Ethernet merece la pena utilizar PCI.

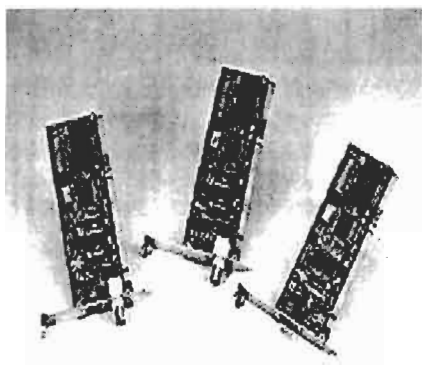


Figura V.1. Vista de algunos tipos de tarjetas de Red.

De todas formas, las tarjetas de red están muy estandarizadas, por lo que no es común encontrar problemas; a muchas tarjetas para Ethernet clásico a veces se las denomina "compatibles con NE2000", una tarjeta de red de Novell que es algo así como el estándar SoundBlaster de las tarjetas de sonido. Otros ordenadores (de marca) incluyen el soporte de red en la placa base, como muchos Dell, Compaq o IBM.

El cableado

Si las redes de ordenadores reciben ese nombre es por los cables. Una red Ethernet puede usar muchos tipos de cables, aunque sólo trataremos dos:

10BASE-2: o bien **RG58**, o **BNC** o **cable coaxial fino**(Figura V.2). Es uno de los cables más clásicos; de un diámetro entorno a 0,5 cm, cada tramo puede tener una longitud máxima de 185 m, con unos 30 ordenadores distribuidos en ese espacio. Es relativamente fácil de usar y montar, aunque resulta algo delicado y puede ser difícil detectar dónde está roto.

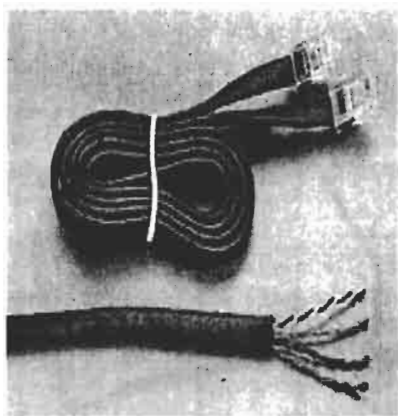


Figura V.2. Diferentes cables utilizados en la conexión de Red.

10BASE-T: o bien UTP, o RJ45 o cable de par trenzado. Externamente es igual que el cable telefónico, incluso en los conectores (las piezas RJ45), aunque no deben confundirse nunca. Con una longitud máxima de unos 100 m por tramo, es muy cómodo de usar, resistente y fácil de diagnosticar errores, aunque necesita usar un aparato denominado **hub** que encarece la compra.

Emplear uno u otro de estos cables depende de varias cosas:

El cable coaxial no permite velocidades de más de **10 Mb/s**, por lo que no puede usarse en redes Fast Ethernet.

El hub es un elemento relativamente caro, unas **10.000 pts** para uno con capacidad para 8 ordenadores; los hubs para Fast Ethernet **suelen ser más caros que los normales**.

Los cables 10BASE-T pueden ser de diversas calidades y tipos (según su nivel o categoría). Para Ethernet basta con cables de nivel 3 con 4 cables interiores; para Fast Ethernet se pueden usar cables **TX**, con 4 cables interiores pero de nivel 5, o bien cables **T4**, de nivel 3, 4 ó 5 pero con 8 cables interiores en vez de 4.

Una **regla práctica** es usar cable coaxial cuando tengamos que conectar un número reducido de ordenadores, 3 ó 4 a lo sumo, y dejar el cable de par trenzado para casos de más ordenadores, o bien muchos en la misma sala o zona, o bien cuando necesitemos la enorme velocidad de Fast Ethernet. Por cierto, el cable para Fast Ethernet se llama a veces "100BASE-..." en alusión a la velocidad de 100 Mb/s de esas redes.

El hub

Como decíamos(Figura V.3), es un elemento que sólo se usa en redes con cables tipo telefónico (10BASE-T, TX, T4...), siendo innecesario en las de cable coaxial. El hub es un elemento de importancia vital, por lo que no conviene regatear en la

Elementos de Arquitectura y Seguridad Informática

compra del mismo, especialmente si queremos comprar uno que soporte redes Fast Ethernet. Físicamente todos los hubs son parecidos:

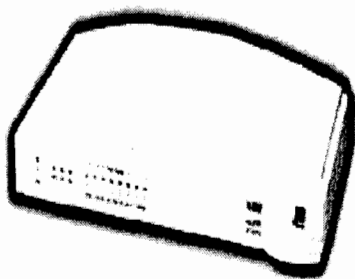


Figura V.3. Hub o Concentrador

Pequeñas cajas de forma rectangular parecidos a módems externos grandes, con numerosos conectores para los cables y una serie de indicadores luminosos que muestran el estado de la red, lo que resulta fundamental a la hora de diagnosticar problemas.

La mayoría de los hubs pueden unirse unos a otros para ampliar la red, aunque para una red del tamaño que nos interesa merece la pena comprar un único hub que gobierne toda la red. Siempre conviene comprar un hub con un par de puertos más de los que necesitamos, ya que así nos ahorraremos dinero y conflictos si decidimos ampliar la red en el futuro.

Servidores y redes punto a punto

En cuanto a la parte lógica, existen dos tipos de redes fundamentalmente: las redes gobernadas por un servidor y las redes punto a punto (peer to peer). El **servidor** es un ordenador de gran potencia y capacidad que actúa de árbitro y juez de la red, la maneja, controla su seguridad y distribuye el acceso a los recursos y los datos; por el contrario, en las **redes punto a punto** ningún ordenador está por encima de otro, sino que existe una especie de democracia y los recursos son distribuidos según desee el usuario de cada ordenador.

Las redes con servidor dedicado suelen ser más complejas de manejo, además de que debemos comprar el servidor, que es un ordenador especial y bastante caro, tanto en hardware (cientos de MBs de memoria, grandes discos SCSI...) como en software especializado (Microsoft Windows NT para servidores, Novell Netware, UNIX... o bien Linux, que es gratis pero complicado de usar). Sin embargo, en cuanto a seguridad y prestaciones son sin duda las mejores; si tiene que montar una red con más de una docena de ordenadores y/o le preocupa la seguridad, contrate un técnico informático y monte una red de este tipo.

Las redes punto a punto son más sencillas de usar, aunque son más inseguras y absolutamente no recomendables para redes de más de una o dos docenas de ordenadores. Una solución intermedia para redes punto a punto es disponer en la red de un ordenador con más potencia que se dedique exclusivamente a tareas rutinarias como impresión, copias de seguridad o almacenaje de archivos, lo que libera al resto de ordenadores sin necesidad de tener un auténtico servidor.

El software

Una red no es nada más que cuatro cables hasta que no instalamos un software para poder manejarla. El software de red tiene dos partes: el **protocolo** de red, que es algo así como el idioma que van a usar las tarjetas para comunicarse, y el propio **programa** de comunicaciones que traduce nuestras órdenes al lenguaje del protocolo de red.

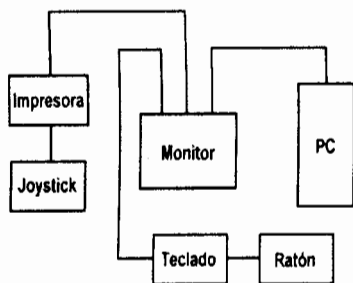
Los protocolos más comunes son el NetBEUI, el IPX/SPX, (Figura V.4) y más recientemente el TCP/IP (que es el que usa la red Internet). En cuanto al programa a usar, dependerá de si nuestro sistema operativo incluye o no soporte para redes. Si lo incluye, deberemos configurarlo para que se comporte como un tipo u otro de **cliente** (para redes tipo Netware, redes tipo Microsoft...); si no lo incluye, deberemos instalar un programa adicional (como Novell Personal Netware para DOS).



Figura V.4. Vista de la instalación de dos protocolos de red el TCP / IP y el NetBEUI de Microsoft.

El USB

USB significa nada menos que Universal Serial Bus, bus serie universal; que sirve para conectar cualquier periférico al ordenador. Claro que en realidad no se trata de cualquier periférico, sino más bien de los periféricos externos típicos: ratón, teclado, joystick, impresora, módem...



Ejemplo de conexiones mediante USB

Figura V.5.

Así que aunque no sea del todo universal, resulta bastante cómodo. Una de sus peculiaridades consiste en que los **hasta 126 dispositivos** (aparte del propio ordenador) van conectados o bien en línea uno detrás de otro (por ejemplo, el PC a la impresora, el módem a la impresora, el ratón al módem...) o bien a unos dispositivos con diversas salidas de conector que pueden estar en cualquiera de los periféricos de la cadena, en el PC o en otros dispositivos como el monitor.

Con el bus USB nos acercaremos más a la auténtica realidad del **P&P** (Figura V.5)

(Plug and Play, enchufar un dispositivo y listo), e incluso algunos dispositivos podrán instalarse sin necesidad de reiniciar el sistema. Claro está que esto dependerá de que los dispositivos y el sistema operativo cooperen adecuadamente, lo cual está por ver; el P&P tiene ya bastantes años y aún da múltiples problemas...

El motivo de que no podamos conectar dispositivos como un disco duro o un CD-ROM al bus USB se debe a su **ancho de banda**: 12 Mb/s, o lo que es lo mismo: **1,5 MBytes/s**. Esto es suficiente para una impresora, que como mucho transmite 1 MB/s, o para un módem (menos de 0,01 MB/s), y no digamos para un ratón o un joystick. Pero un disco duro transmite varios megas por segundo, lo cual lo hace totalmente inadecuado para el bus USB.

Además, el ancho de banda debe repartirse entre los dispositivos, lo que no importa mucho si estamos conectando otro ratón, pero que nos indica que conectar 126 impresoras al mismo puerto USB e intentar imprimir en todas a la vez no es una buena idea. Sin embargo, parece un ancho suficiente para utilizar algunos dispositivos portátiles como las unidades Zip, mientras no intentemos usarlos a la vez que una impresora, un módem y un escáner USB (combinación ciertamente improbable).

Uno de los lugares típicos donde encontraremos conectores USB (Figura V.6) será el monitor, lo que no implica que éste sea un dispositivo USB.

Por último, vamos a evaluar el futuro de esta tecnología. La falta de soporte para ella en Windows 95 ha hecho que haya pasado desapercibida los últimos años, pero la llegada de Windows 98, que sí la soporta, se supone que va a revitalizarla en gran medida.

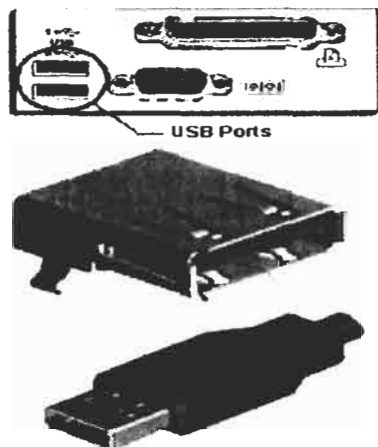


Figura V.6. Vistas de conectores USB

En último término, parece que para los ratones y demás **el futuro pasa inevitablemente por el USB.**

Se debe tener en cuenta que los puertos serie y paralelo son **uno de los estándares** en que se han basado casi 20 años de la vida de los PCs, y **no pueden eliminarse de un plumazo**; nadie va a obviar el hecho de que el 100% de los PCs disponen de estos puertos, o que el 99,99% de las impresoras personales **usan el puerto paralelo** para conectarse con el PC.

VI. Tratamiento de los ficheros de sistema y su explotación

Windows y la memoria virtual

Por supuesto, cuantos más programas utilicemos y más complejos sean, más memoria necesitaremos; esto seguro que no sorprenderá a nadie, pero lo que sí puede que le sorprenda es la gran cantidad de memoria que se utiliza tan sólo para arrancar el sistema operativo. (Ver Tabla VI-1)

¿Impresionado? Como puede ver, sólo la carga del sistema operativo puede consumir TODA la memoria con la que se venden algunos ordenadores de gama baja. Además, Windows 98 utiliza más memoria que Windows 95 debido entre otros temas a su integración con Microsoft Internet Explorer... algo de lo que tal vez Microsoft se arrepienta ahora, vistos sus problemas con los tribunales.

Observen los siguientes datos:

Tabla VI-1

Programas cargados	RAM utilizada
Sólo Windows 95	21 MB
Sólo Windows 98	27 MB
Sólo Windows 98, tras varios meses de funcionamiento y diversas instalaciones de programas	35 MB
Windows 98, Microsoft Word 97 e Internet Explorer 4	46 MB
Windows 98 y AutoCAD 14 (con un dibujo sencillo en 2D)	55 MB

Para terminar de complicar el tema, ambos Windows tienden a aumentar su tamaño y su consumo de memoria según vamos instalando programas... o sencillamente según pasa el tiempo, sin instalar nada.

Pese a esto, el hecho es que los ordenadores siguen trabajando cuando se les agota la memoria RAM, algo que sería imposible si no fuera por la denominada "**memoria virtual**", que no es sino **espacio del disco duro que se utiliza como si fuera memoria RAM**.

Sin embargo, esta memoria virtual tiene varios inconvenientes; el principal es su velocidad, ya que **es muchísimo más lenta que la RAM**. Mientras la velocidad de acceso a la RAM se mide en nanosegundos (ns, la 0,00000001 parte de un segundo), la de los discos duros se mide en milisegundos; es decir, que se tarda casi

un millón de veces más en acceder a un dato que encuentra en el disco duro que a uno de la RAM.

Además, el ancho de banda es también muy inferior; por ejemplo, en un ordenador con memoria PC100 cada segundo pueden transmitirse 800 MB de datos que se encuentren en dicha memoria, mientras que ningún disco duro actual alcanza siquiera los 40 MB/s. Por no hablar del considerable ruido que organizan algunos discos duros, su elevado consumo, y lo más importante: el hecho innegable y no pocas veces lamentado de **la escasa estabilidad de Windows cuando realmente sobrecargamos el "archivo de intercambio"** (el que almacena los datos de la memoria virtual).

Por todo ello, lo ideal es necesitar lo menos posible la memoria virtual, y para eso evidentemente hay que tener la mayor cantidad de memoria RAM posible.

¿Cuánta memoria se está utilizando?

Existen infinidad de métodos para determinarlo; uno de los mejores es el **Monitor del sistema** (Figura VI.1), una de las utilidades incluidas en Windows que, si se ha instalado, se encontrará en la carpeta Accesorios -> Herramientas del sistema. Además, tiene la ventaja de que podemos configurarlo para que nos muestre el tamaño del archivo de intercambio en uso y una infinidad de otros datos, sin consumir él mismo demasiada memoria.

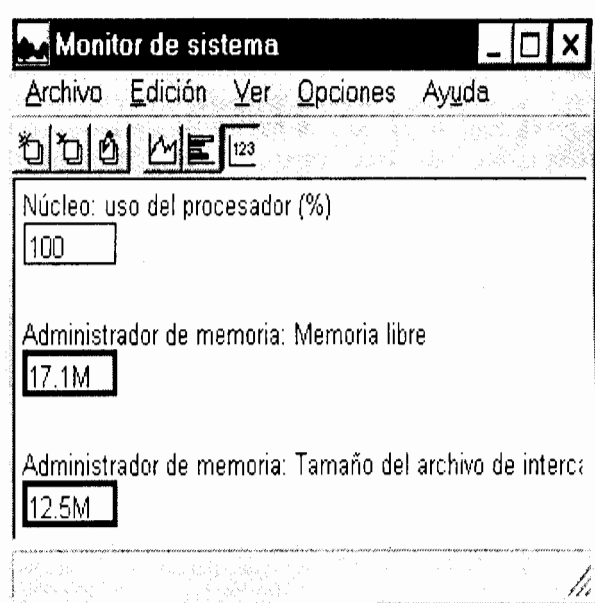


Figura VI.1. Vista del monitor del sistema de Windows.

También podríamos utilizar programas de diagnóstico del PC más complejos, como el excelente Sandra 2000 .

Elementos de Arquitectura y Seguridad Informática

Algunas pruebas de rendimiento

Para ilustrar la importancia de la cantidad de memoria hemos realizado unas cuantas pruebas basadas en la suite Microsoft Office incluida con el programa Winstone 99, centradas no en la puntuación sino en lo que más nota el usuario: el tiempo que se tarda en hacer la prueba (descontando la carga en sí de los programas, por ser independiente de la cantidad de memoria instalada).

Tabla VI-2

RAM instalada	Tiempo empleado
32 MB	466 segundos
48 MB	368 segundos
64 MB	327 segundos
96 MB	307 segundos
128 MB	306 segundos

Configuración: Windows 98, Celeron 466, disco duro UltraDMA33, tarjeta gráfica i740
(podríamos decir que se trata de un ordenador bastante "típico", ni lento ni excesivamente rápido)

Como puede observarse, a partir de 96 MB apenas existe variación en las cifras, pero **pasar de 32 a 64 MB supone un aumento del rendimiento de nada menos que el 42,5%**, y pasar de 64 a 128 MB un aumento adicional del 6,9%. Tenga en cuenta que esto es un test, no la "vida real", pero de cualquier modo no hay duda de que **trabajar con sólo 32 MB en Windows 98 es casi una locura.**

Un EXCESO de memoria no aumenta PARA NADA el rendimiento, sólo se apreciará mejoría si necesitábamos más memoria. Así que si ya tiene 48 MB o más y hace un uso exclusivamente doméstico u ofimático del PC, no se moleste en instalar más.

Consejos y conclusiones

Bueno, ya está bien de teorías; pasemos a la acción. Si va a comprar un ordenador nuevo:

ni se plantee instalar menos de **64 MB**, y si le es posible procure que sean 128 MB;

pida que sea memoria SDRAM **PC133**, a poder ser de una marca conocida, para facilitar las actualizaciones futuras;

sea la cantidad que sea, que venga en el menor número de módulos posible (nada de 2 módulos de 64 MB, mejor 1 de 128);

investigue el número de ranuras que tiene la placa base; al menos deberán ser 3 ranuras, o bien 4 en ordenadores destinados a servidor o estación de trabajo.

Si ya tiene ordenador, éste es un momento tan bueno como cualquier otro para plantearse una ampliación de la memoria. Tenga en cuenta que:

si se trata de un 486 o uno de los primeros Pentium, con memoria FPM, tal vez lo mejor sea no ampliar, o hacerlo con memoria de segunda mano. En todo caso piense que su vida útil no será muy larga.-

en el caso de utilizar memoria EDO (típica de la época del Pentium MMX), todavía puede encontrar módulos nuevos, aunque si los compra de segunda mano tal vez ahorre bastante. No actualice si el PC no es medianamente rápido; y si tiene que quitar unos módulos de poco tamaño para instalar otros de 16 ó 32 MB, adelante;

atención: los chipsets FX, VX y TX para placas Pentium no pueden cachear más de 64 MB de RAM, por lo que superar esa cifra puede implicar una cierta bajada de velocidad, téngalo en cuenta;

si el ordenador utiliza ya memoria SDRAM, bien a 66 ó 100 MHz ("PC66" o "PC100"), intente instalar memoria **PC133**, bien junto a la interior o sustituyéndola por otra;

existen placas con ranuras SIMM (para EDO) y DIMM (para SDRAM), y aunque en teoría se pueden mezclar ambos tipos (y mucha gente lo ha hecho), algunas personas recomiendan no hacerlo.

Por cierto, en ordenadores "antiguos" con ranuras DIMM, generalmente Pentium MMX o los primeros Pentium II, a menudo resulta problemático instalar módulos de memoria modernos de PC100 o PC133, por muy diversos y discutidos motivos (tamaño de los módulos, número de caras de los mismos, velocidades de acceso, incompatibilidades específicas del chipset o la placa base...)

En el futuro la tendencia parece que no va a cambiar: **cada vez necesitaremos más memoria** (Windows 2000 ya "recomienda" 64 MB y añade que cualquier aumento sobre esta cantidad mejorará el rendimiento), y no sería raro que antes de un año los ordenadores vinieran como mínimo con 128 MB, en lugar de 32. Y eso pese a la famosa frase de Bill Gates en los comienzos de la era PC: "nadie debería necesitar más de 640 KB de memoria"... para el que no lo sepa, 640 KB son nada menos que 0,625 MB.

VII. Equipos periféricos asociados

Puertos series (UART)

Se trata del chip que controla los puertos serie del ordenador. En el caso de los módems internos no tiene especial importancia, ya que suelen traer la suya, preparada para la velocidad que necesitan. Los externos, sin embargo, puesto que se conectan a uno de los puertos COM ya existentes en el ordenador, dependen de la velocidad de la UART de éste.

Las UART se designan con un número de referencia. Si bien han existido varios modelos en los casi veinte años de vida de los PCs, los más comunes han sido el 8250 y el 16550. La **8250** es el modelo clásico, que se usó hasta mediada la vida de los 486; es capaz de manejar sin problemas módems hasta de 14.400 baudios, pero resulta insuficiente para módems más rápidos.

La **16550** es un modelo mucho más avanzado que llega a proporcionar velocidades internas PC-módem de hasta 115.200 baudios, más que suficientes para módems de 28.800, 33.600 y 55.600 baudios. Además de un diseño más complejo, tiene buffers de memoria en los que guardar información hasta que pueda ser procesada.

Otros modelos son la 16540, que es un modelo de transición entre ambas y que como mucho puede manejar módems de 28.800 baudios, aunque ya con ciertas mermas de rendimiento, y las diversas variantes y mejoras de la 16550 (16550AF y muchas otras de número de referencia superior).

Para identificar el modelo de UART presente en un ordenador se suelen usar programas software que detectan el hardware, aunque los resultados no siempre son exactos. Uno de estos programas es el MSD de Microsoft, que viene con las últimas versiones del DOS, así como en el CD de Windows 95 (si bien no se instala por defecto y debe hacerse a mano).

Tanto en el MSD como en otros programas, si el programa detecta una UART 16550 o superior es casi seguro que ha acertado; sin embargo, si detecta una 8250 puede que no sea correcto y en realidad sea un modelo más avanzado. Otros programas que detectan el hardware del ordenador son CheckIt, Agsi, PCConfig o Hardware Info; todos ellos pueden localizarse y obtenerse en Internet, en la dirección www.shareware.com o bien mediante Yahoo u otros buscadores.

Para cambiar una UART que resulta insuficiente para instalar un módem externo de cierta velocidad, deberemos cambiar la tarjeta que controla los puertos COM. En dicha tarjeta, generalmente ISA, es donde se encontrará la UART y los chips para el soporte de puerto paralelo, así como en ocasiones para la disquetera y los discos duros IDE. En los ordenadores más modernos estas habilidades vienen integradas en la placa base, o al menos el soporte para discos duros. En muchos casos no hará falta sustituir la tarjeta, sino que bastará con deshabilitar mediante unos jumpers en

la misma el soporte de puertos COM y habilitarlo en la nueva tarjeta, que añadiríamos sin quitar la antigua. Estas tarjetas (también conocidas como de I/O) son muy baratas, menos de 5.000 pts, pero resultan cada vez más difíciles de encontrar debido a la integración de estos componentes en la placa base.

Por cierto, existen criterios que algunos módems internos carecen de UART o bien no la configuran adecuadamente, por lo que es como si no existiera e intentan usar la del ordenador, lo que puede dar problemas de rendimiento, de conflicto entre dispositivos o complicar la configuración del módem.

Puerto paralelo

Es el método más común de conexión para escáners **domésticos**, entendiendo como tales aquellos de resolución intermedia-alta (hasta 600x1.200 ppp, pero más comúnmente de 300x600 ó 400x800 ppp) en los que la velocidad no tiene necesidad de ser muy elevada mientras que el precio es un factor muy importante.

El puerto paralelo, a veces denominado LPT1, es el que utilizan la mayor parte de las impresoras; como generalmente el usuario tiene ya una conectada a su ordenador, el escáner tendrá dos conectores, uno de entrada y otro de salida, de forma que quede conectado en medio del ordenador y la impresora. Como primer problema de este tipo de conexión tenemos el hecho de que arbitrar el uso del puerto paralelo es algo casi imposible, por lo que en general no podremos imprimir y escanear a la vez (aunque para un usuario doméstico esto no debería ser excesivo problema).

De cualquier modo, debemos tener presente el hecho de que para obtener una velocidad razonable, el puerto debe estar configurado en los **modos ECP o EPP** (dependiendo del escáner en concreto), lo cual se selecciona generalmente en la BIOS. El problema aparece cuando el ordenador que queremos conectar es algo antiguo y no puede configurar el puerto más que en el antiguo estándar, 10 veces más lento (como ocurre con los primeros 486 e inferiores), o cuando surgen conflictos con otros dispositivos que tengamos conectados al puerto paralelo, como unidades Zip o algunas impresoras modernas.

En estos casos puede merecer la pena comprar una tarjeta controladora nueva que sustituya al puerto actual o bien que añada un segundo puerto (que será LPT2); estas tarjetas controladoras de dispositivos, llamadas también de I/O, son baratas pero en ocasiones difíciles de encontrar por estar en la actualidad integradas en la placa base.

Teclado

El teclado (Figura VII.1) es un componente al que se le da poca importancia, especialmente en los ordenadores clónicos. Si embargo es un componente esencial, pues es el que permitirá que nuestra relación con el ordenador sea fluida y

Elementos de Arquitectura y Seguridad Informática

agradable, de hecho, junto con el ratón son los responsables de que podamos interactuar con nuestra máquina.

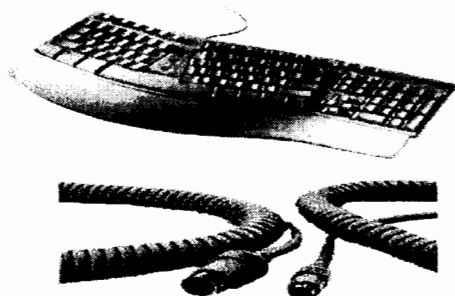


Figura VII.1. Vista de un teclado y dos tipos de conectores DIN y Mini DIN

Así, si habitualmente usamos el procesador de textos, hacemos programación, u alguna otra actividad en la que hagamos un uso intensivo de este componente, es importante escoger un modelo de calidad. En el caso de que seamos usuarios esporádicos de las teclas, porque nos dediquemos más a juegos o a programas gráficos, entonces cualquier modelo nos servirá, eso sí, que sea de tipo mecánico. No acepteis ningún otro.

Parámetros importantes a tener en cuenta son el tacto, no debe de ser gomoso, y el recorrido, no debe de ser muy corto. También es importante la ergonomía, es aconsejable que disponga de una amplia zona en la parte anterior, para poder descansar las muñecas. Y hablando de la ergonomía, este es uno de los parámetros que más destaca en un teclado, uno de los ya clásicos en este aspecto es el "Natural keyboard" de Microsoft.

Y ya pasando a aspectos más técnicos, vamos a describir en detalle sus características. Actualmente sólo quedan dos estándares en cuanto a la distribución de las teclas, el expandido, que IBM lo introdujo ya en sus modelos AT, y el de Windows95, que no es más que una adaptación del extendido, al que se le han añadido tres teclas de más, que habitualmente no se usan, y que sólo sirven para acortar la barra espaciadora hasta límites ridículos.

En cuanto al conector, también son dos los estándares, el DIN, y el mini-DIN. El primero es el clásico de toda la vida, y aún es el habitual en equipos clónicos.

El segundo, introducido por IBM en sus modelos PS/2, es usado por los fabricantes "de marca" desde hace tiempo, y es el habitual en las placas con formato ATX.

De todas formas, no es un aspecto preocupante, pues hay convertidores de un tipo a otro.

Nos dejamos otro tipo de conector cada vez más habitual, el **USB**, pero la verdad es que de momento apenas hay teclados que sigan este estandar.

¿Qué es... un escáner?

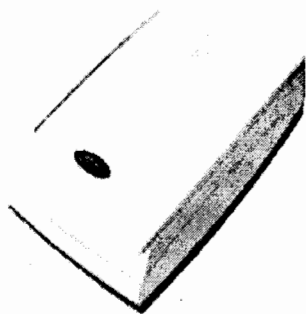


Figura VII.2. Vista de Escáner

Ateniéndonos a los criterios de la Real Academia de la Lengua, digamos que es la palabra que se utiliza en informática para designar a un aparato **digitalizador de imagen**.

Por digitalizar se entiende la operación de transformar algo analógico (algo físico, real, de precisión infinita) en algo digital (un conjunto finito y de precisión determinada de unidades lógicas denominadas bits). En fin, en el caso que nos ocupa se trata de coger una imagen (fotografía, dibujo o texto) y convertirla a un formato que podamos almacenar y modificar con el ordenador.

Realmente un escáner (Figura VII.2) no es ni más ni menos que los ojos del ordenador.

Cómo funciona

El proceso de captación de una imagen resulta casi idéntico para cualquier escáner: se ilumina la imagen con un foco de luz, se conduce mediante espejos la luz reflejada hacia un dispositivo denominado CCD que transforma la luz en señales eléctricas, se transforma dichas señales eléctricas a formato digital en un DAC (convertor analógico-digital) y se transmite el caudal de bits resultante al ordenador.

El **CCD** (Charge Coupled Device, dispositivo acoplado por carga -eléctrica-) es el elemento fundamental de todo escáner, independientemente de su forma, tamaño o mecánica. Consiste en un elemento electrónico que reacciona ante la luz, transmitiendo más o menos electricidad según sea la intensidad y el color de la luz que recibe; es un auténtico ojo electrónico.

La calidad final del escaneado dependerá fundamentalmente de la calidad del CCD; los demás elementos podrán hacer un trabajo mejor o peor, pero si la imagen no es captada con fidelidad cualquier operación posterior no podrá arreglar el problema. Teniendo en cuenta lo anterior, también debemos tener en cuenta la calidad del DAC, puesto que de nada sirve captar la luz con enorme precisión si perdemos mucha de esa información al transformar el caudal eléctrico a bits.

La resolución

No podemos continuar la explicación sin definir este término, uno de los parámetros más utilizados (a veces incluso demasiado) a la hora de determinar la calidad de un escáner. La resolución (medida en **ppp**, puntos por pulgada) puede

definirse como el número de puntos individuales de una imagen que es capaz de captar un escáner... aunque en realidad no es algo tan sencillo.

La resolución así definida sería la **resolución óptica o real** del escáner. Así, cuando hablamos de un escáner con resolución de "300x600 ppp" nos estamos refiriendo a que en cada línea horizontal de una pulgada de largo (2,54 cm) puede captar 300 puntos individuales, mientras que en vertical llega hasta los 600 puntos; como en este caso, generalmente la resolución horizontal y la vertical no coinciden, siendo mayor (típicamente el doble) la vertical.

Esta resolución óptica viene dada por el CCD y es la más importante, ya que implica los límites físicos de calidad que podemos conseguir con el escáner. Por ello, es un método comercial muy típico comentar sólo el mayor de los dos valores, describiendo como "un escáner de 600 ppp" a un aparato de 300x600 ppp o "un escáner de 1.200 ppp" a un aparato de 600x1.200 ppp; téngalo en cuenta, la diferencia es obtener o no el cuádruple de puntos.

Tenemos también la **resolución interpolada**; consiste en superar los límites que impone la resolución óptica (300x600 ppp, por ejemplo) mediante la estimación matemática de cuáles podrían ser los valores de los puntos que añadimos por software a la imagen. Por ejemplo, si el escáner capta físicamente dos puntos contiguos, uno blanco y otro negro, supondrá que de haber podido captar un punto extra entre ambos sería de algún tono de gris. De esta forma podemos llegar a resoluciones absurdamente altas, de hasta 9.600x9.600 ppp, aunque en realidad no obtenemos más información real que la que proporciona la resolución óptica máxima del aparato. Evidentemente este valor es el que más gusta a los anunciantes de escáners...

Por último está la propia **resolución de escaneado**, aquella que seleccionamos para captar una imagen concreta. Su valor irá desde un cierto mínimo (típicamente unos 75 ppp) hasta el máximo de la resolución interpolada. En este caso el valor es siempre idéntico para la resolución horizontal y la vertical, ya que si no la imagen tuviese las dimensiones deformadas.

Los colores y los bits

Al hablar de imágenes, digitales o no, a nadie se le escapa la importancia que tiene el color. Una fotografía en color resulta mucho más agradable de ver que otra en tonos grises; un gráfico acertadamente coloreado resulta mucho más interesante que otro en blanco y negro; incluso un texto en el que los epígrafes o las conclusiones tengan un color destacado resulta menos monótono e invita a su lectura.

Sin embargo, digitalizar los infinitos matices que puede haber en una foto cualquiera no es un proceso sencillo. Hasta no hace mucho, los escáners captaban las imágenes únicamente en blanco y negro o, como mucho, con un número muy limitado de matices de gris, entre 16 y 256. Posteriormente aparecieron escáners que podían captar color, aunque el proceso requería tres pasadas por encima de la imagen, una para cada color primario (rojo, azul y verde). Hoy en día la práctica

Elementos de Arquitectura y Seguridad Informática

totalidad de los escáners captan hasta 16,7 millones de colores distintos en una única pasada, e incluso algunos llegan hasta los 68.719 millones de colores.

Para entender cómo se llega a estas apabullantes cifras debemos explicar cómo asignan los ordenadores los colores a las imágenes. En todos los ordenadores se utiliza lo que se denomina sistema binario, que es un sistema matemático en el cual la unidad superior no es el 10 como en el sistema decimal al que estamos acostumbrados, sino el 2. Un bit cualquiera puede por tanto tomar 2 valores, que pueden representar colores (blanco y negro, por ejemplo); si en vez de un bit tenemos 8, los posibles valores son 2 elevado a 8 = 256 colores; si son 16 bits, 2 elevado a 16 = 65.536 colores; si son 24 bits, 2 elevado a 24 = 16.777216 colores; etc, etc.

Por tanto, "**una imagen a 24 bits de color**" es una imagen en la cual cada punto puede tener hasta 16,7 millones de colores distintos; esta cantidad de colores se considera suficiente para casi todos los usos normales de una imagen, por lo que se le suele denominar **color real**. La casi totalidad de los escáners actuales capturan las imágenes con 24 bits, pero la tendencia actual consiste en escanear incluso con más bits, 30 ó incluso 36, de tal forma que se capte un espectro de colores absolutamente fiel al real; sin embargo, casi siempre se reduce posteriormente esta profundidad de color a 24 bits para mantener un tamaño de memoria razonable, pero la calidad final sigue siendo muy alta ya que sólo se eliminan los datos de color más redundantes.

¿Cuánto ocupa una imagen?

Depende de la imagen. Para saber exactamente cuál va a ser el tamaño de una imagen, deberemos usar la siguiente fórmula:

$$\text{Tamaño imagen (KB)} = L \times A \times RH \times RV \times \text{bits} / 8.192$$

Donde L y A son las dimensiones de la imagen en pulgadas (una pulgada = 2,54 cm) y RH y RV las resoluciones horizontal y vertical respectivamente. Hagamos un ejemplo rápido: una imagen DIN-A4 (aproximadamente 11,7x8,3 pulgadas) escaneada a 300 ppp (300x300) con 24 bits de color (color real) ocupa ¡**25.490 KB!!** (unos **25 MB**, 25 megas!!). La cifra resulta impactante, pero no se preocupe; existen muchos métodos para reducir el tamaño de las imágenes, tanto a la hora de manejarlas en memoria como a la de almacenarlas en el disco duro.

El primer método consiste en **escanear a menor resolución**; la calidad es menor, pero el tamaño del fichero resultante también. Si la imagen va a tener como destino la pantalla de un ordenador, 75 ppp serán casi siempre suficientes, lo que reduciría el tamaño de la imagen anterior a apenas 1.593 KB, poco más de 1,5 MB.

Como segundo método tenemos **reducir la profundidad de color**. Si la imagen anterior es un dibujo a tinta china, con escanear a 1 bit (en blanco y negro) puede que tengamos suficiente. Esto reduciría el tamaño a tan sólo 1.062 KB, casi exactamente 1 MB.

Por último podemos **archivar la imagen en formato comprimido**. En este caso el tamaño de la imagen en memoria permanece invariable (25 MB), pero el tamaño en disco puede quedar en menos de una quinta parte sin pérdida de calidad, o incluso menos si la compresión se realiza eliminando información redundante. Como ejemplo de formatos de archivo de imagen con compresión tenemos los JPEG (o JPG), GIF o TIFF, frente al clásico BMP que carece de compresión alguna.

Lo más importante es que podemos combinar los factores anteriores para conseguir resultados realmente optimizados; así, escaneando la imagen del ejemplo a 75 ppp, con 1 bit de color y guardándola en formato GIF, el resultado puede ocupar **tan sólo 66 KB en memoria y menos de 15 KB en disco**.

Cabe destacar que en muchos casos se utilizan escalas de 256 grises (8 bits) para representar más fielmente originales en blanco y negro con bordes muy definidos o pequeños tamaños de letra. Sobre qué es el OCR trataremos a continuación, se trata de una de las aplicaciones más comunes de los escáners. OCR son las siglas de Optical Character Recognition, reconocimiento óptico de caracteres, o con una descripción más sencilla: cómo hacer para enseñar a leer al ordenador.

Si pensamos un poco en el proceso de escaneado que hemos descrito anteriormente, nos daremos cuenta de que al escanear un texto no se escanean letras, palabras y frases, sino sencillamente los puntos que las forman, una especie de fotografía del texto. Evidentemente, esto puede ser útil para archivar textos, pero sería deseable que pudiéramos coger todas esas referencias tan interesantes pero tan pesadas e incorporarlas a nuestro procesador de texto no como una imagen, sino **como texto editable**.

Lo que deseáramos en definitiva sería que el ordenador supiera leer como nosotros. Bueno, pues eso hace el OCR: es un programa que lee esas imágenes digitales y busca conjuntos de puntos que se asemejen a letras, a caracteres. Dependiendo de la complejidad de dicho programa entenderá más o menos tipos de letra, llegando en algunos casos a interpretar la escritura manual, mantener el formato original (columnas, fotos entre el texto...) o a aplicar reglas gramaticales para aumentar la exactitud del proceso de reconocimiento.

Para que el programa pueda realizar estas tareas con una cierta fiabilidad, sin confundir "t" con "1", por ejemplo, la imagen que le proporcionamos debe cumplir unas ciertas características. Fundamentalmente debe tener una **gran resolución**, unos 300 ppp para textos con tipos de letra claros o 600 ppp si se trata de tipos de letra pequeños u originales de poca calidad como periódicos. Por contra, podemos ahorrar en el aspecto del color: casi siempre bastará con blanco y negro (1 bit de color), o a lo sumo una escala de 256 grises (8 bits). Por este motivo algunos escáners de rodillo (muy apropiados para este tipo de tareas) carecen de soporte para color.

Formatos de escáner

Físicamente existen varios tipos de escáner, cada uno con sus ventajas y sus inconvenientes:

De sobremesa o planos: son los modelos más apreciados por su buena relación precio/prestaciones, aunque también son de los periféricos más incómodos de ubicar debido a su gran tamaño; un escáner para DIN-A4 plano puede ocupar casi 50x35 cm, más que muchas impresoras, con el añadido de que casi todo el espacio por encima del mismo debe mantenerse vacío para poder abrir la tapa. Sin embargo, son los modelos más versátiles, permitiendo escanear fotografías, hojas sueltas, periódicos, libros encuadernados e incluso transparencias, diapositivas o negativos con los adaptadores adecuados. Las resoluciones suelen ser elevadas, 300x600 ppp o más, y el precio bastante ajustado. El tamaño de escaneado máximo más común es el DIN-A4, aunque existen modelos para A3 o incluso mayores (aunque ya con precios prohibitivos).

De mano: son los escáners "portátiles", con todo lo bueno y lo malo que implica esto. Hasta hace unos pocos años eran los únicos modelos con precios asequibles para el usuario medio, ya que los de sobremesa eran extremadamente caros; esta situación a cambiado tanto que en la actualidad los escáners de mano están casi en vías de extinción. Descansen en paz. Su extinción se debe a las limitaciones que presentan en cuanto a tamaño del original a escanear (generalmente puede ser tan largo como se quiera, pero de poco más de 10 cm de ancho máximo) y a su baja velocidad, así como a la carencia de color en los modelos más económicos. Lo que es más, casi todos ellos carecen de motor para arrastrar la hoja, sino que es el usuario el que debe pasar el escáner sobre la superficie a escanear (abstenerse aquellos con mal pulso). Todò esto es muy engorroso, pero resulta eficaz para escanear rápidamente fotos de libros encuadernados, artículos periodísticos, facturas y toda clase de pequeñas imágenes sin el estorbo que supone un escáner plano.

De rodillo: unos modelos de aparición relativamente moderna, se basan en un sistema muy similar al de los aparatos de fax: un rodillo de goma motorizado arrastra a la hoja, haciéndola pasar por una rendija donde está situado el elemento captador de imagen. Este sistema implica que los originales sean hojas sueltas, lo que limita mucho su uso al no poder escanear libros encuadernados sin realizar antes una fotocopia (o arrancar las páginas, si se es muy bestia), salvo en modelos peculiares como el Logitech FreeScan que permite separar el cabezal de lectura y usarlo como si fuera un escáner de mano. A favor tienen el hecho de ocupar muy poco espacio, incluso existen modelos que se integran en la parte superior del teclado; en contra tenemos que su resolución rara vez supera los 400x800 puntos, aunque esto es más que suficiente para el tipo de trabajo con hojas sueltas al que van dirigidos.

Modelos especiales: aparte de los híbridos de rodillo y de mano, existen otros escáners destinados a aplicaciones concretas; por ejemplo, los destinados a escanear exclusivamente fotos, negativos o diapositivas, aparatos con resoluciones reales del orden de 3.000x3.000 ppp que muchas veces se asemejan más a un CD-ROM (con bandeja y todo) que a un escáner clásico; o bien los bolígrafos-escáner, utensilios con forma y tamaño de lápiz o marcador fluorescente que escanean el texto por encima del cual los pasamos y a veces hasta lo traducen a otro idioma al

instante; o impresoras-escáner, similares a fotocopiadoras o más particulares como las Canon, donde el lector del escáner se instala como un cartucho de tinta.

El Mouse

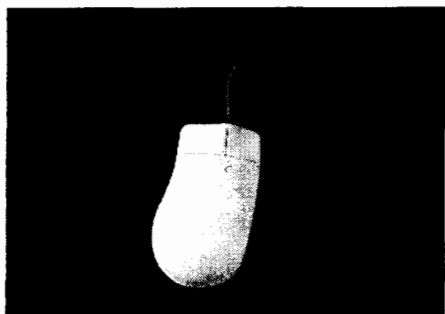


Figura VII.3 Vista de un Mouse

Douglas Engelbart creó el dispositivo conocido como Mouse en el año 1963. Al comienzo de los años 70 la compañía Xerox desarrolló el concepto de Mouse digital que a diferencia del de Engelbart, no usaba resistores variables y circuitos de conversión analógico-digitales.

Muchos de los principios básicos de ese nuevo diseño han sido trasladados al Mouse moderno de las PC (Figura VII.3).

En 1982, Mouse Systems introdujo el primer Mouse para las IBM PC. Con el tiempo, Microsoft también vio al Mouse como un gran dispositivo de gran potencial en el mercado de la PC y como compañía de software que poseía los medios para fomentar su uso, desarrolló el software que lo soportara. Así Microsoft introdujo su Mouse de dos botones. Con la subsiguiente introducción de programas, como Microsoft Word, Excel y Windows, mostraba a los usuarios de las Pc que el Mouse podía trabajar con las computadoras, fácil y eficientemente.

Existen más Mouse en las PC que cualquiera de los otros dispositivos de selección alternativos (Track-balls, Tabletas gráficas, Light Pens y Pantallas sensibles al tacto)

¿Por qué el Mouse?

El Mouse, cuyo nombre parte de los primeros modelos por la semejanza de sus formas con las de este roedor, ha tenido en los últimos tiempos una fuerte expansión, debido a su propia evolución hacia formas más ergonómicas y fáciles de operar. Sin embargo, la verdadera expansión del Mouse se registra por la proliferación de las Interfaces Gráficas de Usuario (GUI), en las que se aprecian las cualidades que éste brindaba para la gestión de un sistema microinformático. Por medio del GUI y el Mouse, el usuario posee el control total de la computadora, sin necesidad de pulsar una sola tecla o tener que recurrir a los comandos siempre difíciles de memorizar.

Tecnología y Funcionamiento

La arquitectura de un Mouse resulta muy sencilla y existen básicamente cuatro tipos de Mouse, que se clasifican de acuerdo con el tipo de mecanismo que se emplean para transmitir sus movimientos a la computadora, estos son:

1. De bola.
2. De rodillos.
3. Opto electrónico.
4. Óptico.

Mouse de bola

Este es más común y sencillo. Se basa en una bola recubierta por una sustancia adherente que entra en contacto con la mesa de trabajo. Al moverlo por la superficie, la bola gira en todos los sentidos posibles y transmite así su movimiento a dos rodillos mecánicos situados en el interior de la carcasa. De éstos, uno se encarga de recoger los desplazamientos horizontales y el otro, los verticales, determinando el movimiento diagonal. Ambos están conectados a dos codificadores digitales que se encargan de transformar el movimiento en impulsos eléctricos que serán enviados a la computadora.

Un DRIVER (Controlador) residente en memoria o cargado cada vez que se utiliza una determinada aplicación, será el que interprete estos impulsos y a su vez los convertirá en posiciones del cursor en la pantalla.

Mouse de rodillos

El mecanismo de este tipo de Mouse es el mismo que el de bolas, con la diferencia de que desaparece la bola y queda sustituida directamente por los rodillos que entran en contacto directo con la superficie de desplazamiento. Con ello se consigue simplificar aún más el mecanismo y reducir los costos de fabricación del dispositivo.

Mouse opto electrónico

Como su nombre indica, emplea técnicas mecánicas y ópticas para transmitir los desplazamientos a la computadora. Dispone en su interior de dos emisores y dos detectores de luz, enfrentados uno a uno, que se encargan de transmitir los movimientos horizontales y verticales, respectivamente. Su uso requiere de una superficie especial que permita producir desviaciones en la luz procedente de los emisores. Por ello son suministrados, bien con una placa metálica que tiene grabada una finísima retícula. El movimiento del mouse en esta superficie es recogido por un disco que posee diversos agujeros de forma que se permita el paso de la luz a determinados intervalos.

Mouse óptico

Son mucho más complejos y en ellos es imprescindible una superficie especial para efectuar los desplazamientos. Se trata de dispositivos que disponen de dos emisores de luz infrarroja y dos celdas fotosensibles. La placa metálica es una malla impresa, de forma que se determinan unas zonas opacas y otras brillantes; de esta manera,

los emisores de luz lanzan su rayo luminoso sobre la placa, que se refleja, y son captados a continuación por los receptores.

Cuando el haz es proyectado sobre una zona opaca no se produce reflexión, lo cual es interpretado por los receptores como una señal eléctrica. La detección de esa falta de reflexión por uno u otros de los receptores se determina como un movimiento horizontal o vertical, en dependencia de cuál de ellos la registre.

¿Cómo se comunica el Mouse con la computadora?

El Mouse puede estar conectado a la computadora por medio de un cable enchufado a la interfaz serie RS-232C (Denominados **tipo serie**), que es el mismo que se utiliza para la transmisión de datos o bien a una placa especial en uno de los Slots de expansión. Por otro lado, el tipo serie dispone de grandes ventajas, ya que la conexión es mucho más sencilla y su costo es inferior. En algunos modelos el cable desaparece al quedar sustituido por un emisor y un receptor infrarrojos. Como se observa, el mecanismo descrito es realmente sencillo, lo que hace de este periférico un dispositivo verdaderamente fiable.

En los de bola, el único inconveniente es la suciedad que se acumula sobre la superficie de este elemento, lo que dificulta una transmisión eficiente de sus movimientos a los rodillos. Para evitar esta situación es necesario limpiarla frecuentemente, también es conveniente disponer de una alfombrilla. (Pad)

A diferencia del modelo serial, el mouse bus no contiene su propio microprocesador, en su lugar, la tarjeta es la encargada de monitorear al mouse y notificar al Driver cuándo ocurrió un evento sobre él. En la mayoría de las implementaciones, la tarjeta es programada con el fin de encuestar a intervalos regulares al mouse (11/30 a 1/60 segundos), e interrumpir al microprocesador de forma que el Driver pueda leer su estado desde los registros en la tarjeta.

Esta tasa de interrupciones está determinada porque entre 30 y 60 Hz se encuentra la mayoría de las tasas de refrescamiento de los monitores. Otro tipo de interfaz es el de las computadoras PS/2. Estas siglas corresponden a los equipos fabricados por IBM, que salió al mercado con las 386 y que significa **Personal System 2**, en el año 1987.

Este mouse es similar al serial en muchas cuestiones. Contiene un microprocesador que transmite datos seriales al controlador del teclado dentro de la PS/2. Este decodifica esa información y el BIOS la hace disponible al DRIVER.

La resolución

La resolución de un Mouse se refiere al número de puntos que éste puede detectar por cada pulgada de movimiento. Una de las características más importantes en un mouse la resolución. Este parámetro indica la relación existente entre el movimiento del mismo sobre la superficie de la mesa y equivalente en desplazamientos del cursor en la pantalla.

¿Qué es... un monitor?

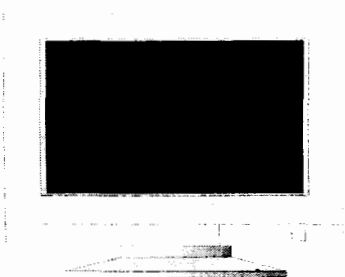


Figura VII.4 Vista de un Monitor.

Evidentemente, es la pantalla en la que se ve la información suministrada por el ordenador (Figura VII.4). En el caso más habitual se trata de un aparato basado en un tubo de rayos catódicos (CRT) como el de los televisores, mientras que en los portátiles es una pantalla plana de cristal líquido (LCD).

Si alguna vez se ha enfrentado al manual de su monitor (para lo que demasiadas veces hace falta saber inglés, alemán o japonés, ya que rara vez vienen en otro idioma), habrá

encontrado un galimatías impresionante sobre Hz, MHz, refresh y demás aspectos. Usted intuye que eso tiene que ver con la calidad del aparato, pero ¿qué significa? Vamos a intentar explicarlo.

Los bloques principales que conforman al monitor son: (Figura VII.5)

1. CRT. Tubo de rayos catódicos.
2. Amplificador de video.
3. Circuito de deflexión y sincronización horizontal y vertical.
4. Fuente de alimentación.

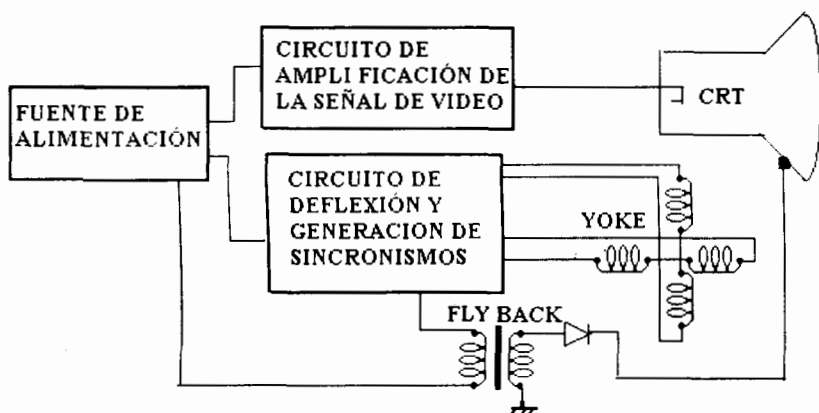


Figura VII.5. Esquema 1: Diagrama en bloques de los monitores.

MODO DE TRABAJO, los diferentes tipos de monitores que pueden utilizarse con las microcomputadoras son:

1. Monitores **Monocromos** Direct-drive .Obsoletos, diseñados para trabajar con la tarjeta monocroma MDA (Monocromo Drive Adapter). También pueden utilizarse con la EGA.
2. Monitores Monocromos Compuestos. Se conectan a la salida de vídeo compuesto del controlador CGA y proporcionan una imagen de un solo color bastante aceptable.
3. **CGA**, se conectan al controlador Color Graphics Adapter .Combinan la alta calidad de las pantallas de texto de los monitores monocromos con gráficos de alta resolución y colores. También conocidos como RGB que significa Red-Green-Blue, porque utilizan estas 3 señales separadas.
4. **EGA**, controlados por la tarjeta Enhanced Graphics Adapter. Permiten una paleta de 64 colores máximo. Son multisíncronos lo que les permite ajustarse a las diferentes señales generadas por las tarjetas CGA y EGA.
5. **VGA**, Video Graphics Adapter / Video Graphics Array; en estos monitores las señales de video son analógicas (viajan por cables coaxiales), lo que permite representar en pantalla mayor cantidad de colores.

Mejoran la calidad de los gráficos, usan señal analógica con lo que se puede representar un rango continuo de intensidades para cada color. Teóricamente el monitor analógico permite un ilimitado número de colores e intensidades (en la práctica el inevitable ruido y las limitaciones del CRT restringen el número de colores en el orden de los 64- 256 intensidades distinguibles para cada canal).

TAMAÑO. Se mide en número de pulgadas en diagonal, y nos indica el tamaño visible del tubo de imagen. El tamaño del monitor no debe elegirse a la ligera, pues depende directamente de la resolución a la que se vaya a trabajar, aunque también es cierto que a mayor tamaño, mayor número de programas o aplicaciones podremos tener abiertas y visibles simultáneamente en pantalla.

FRECUENCIA DE PUNTOS (ancho de banda de la imagen). Define la cantidad de puntos (pixels) que deben ser iluminados en un segundo, garantizando que la pantalla completa sea barrida en un período del sincronismo vertical. Se calcula multiplicando por (1.5 a 3) el total de pixels y por la frecuencia vertical.

ANCHO DE BANDA DEL MONITOR (PIXEL RATE). Se define así a la capacidad de los circuitos de amplificación de video del monitor de hacer transiciones de ON a OFF sin que disminuya su ganancia. Un monitor que pueda manejar un ancho de banda superior al que requiere la imagen, mostrará a ésta cualitativamente mucho mejor. En el ancho de banda del monitor influyen la calidad de los cables y su largo mínimo aceptable, las terminaciones del conector, el que no hayan extensiones, la estabilidad de la electrónica del monitor y que esté apantallado.

Para el modo VGA es necesario un ancho de banda de 34 Mhz, se alcanzan los 250 Mhz ahora. Gracias al ancho de banda aumentado se pueden proporcionar mayores frecuencias verticales de refrescamiento. En el ancho de banda del monitor influyen la calidad de los cables y su largo mínimo aceptable, las terminaciones del

Elementos de Arquitectura y Seguridad Informática

conector, el que no hayan extensiones, la estabilidad de la electrónica del monitor y que esté apantallado.

Resolución (Resolution)

Se trata del número de puntos que puede representar el monitor por pantalla, en horizontal x vertical. Así, un monitor cuya resolución máxima sea de 1024x768 puntos puede representar hasta 768 líneas horizontales de 1024 puntos cada una, probablemente además de otras resoluciones inferiores, como 640x480 u 800x600.

Cuanto mayor sea la resolución de un monitor, mejor será la calidad de la imagen en pantalla, y mayor será la calidad del monitor. La resolución debe ser apropiada además al tamaño del monitor; es normal que un monitor de 14" ó 15" no ofrezca 1280x1024 puntos, mientras que es el mínimo exigible a uno de 17" o superior.

Es una de las características más importantes de un monitor, indica el número mayor de pixels o puntos que se pueden visualizar en la pantalla. A mayor resolución mayor será el ancho de banda a emplear. En la resolución influyen el ancho de banda de la fuente de video, el cable, los amplificadores de video y el tamaño focal de cada punto del CRT.

Hay unas resoluciones recomendadas para cada tamaño de pantalla. Cuando un monitor tiene un tamaño de punto demasiado grande, se produce un solapamiento en las resoluciones mayores, dando lugar a una pérdida de calidad de la imagen. Si se desea utilizar resoluciones altas no habrá más remedio que comprar un monitor de gran tamaño, en caso contrario no se podrán apreciar los detalles.

Un monitor de 14" es válido para trabajar a resoluciones de 640x480 e incluso a 800x600, aunque en la mayoría de los casos con una notable falta de definición. Un monitor de 15" debe ser un mínimo hoy en día, para poder trabajar cómodamente a 800x600, y ocasionalmente a 1024x768. La primera de ellas es la resolución recomendada para ver la mayoría de las páginas WEB, y en trabajo con aplicaciones estándar nos permite presentar todas las barras de menús e iconos sin que nos ocupen cerca de la mitad de la pantalla visible.

Un monitor de 17" es el monitor ideal por prestaciones y por precio, permite trabajar a 1024x768 e incluso a 1280x1024, esta última sobre todo para el tratamiento de imágenes o para trabajar con dos aplicaciones abiertas simultáneamente. Los monitores de 21" son excesivamente caros, y solamente son necesarios para un trabajo profesional.

La Tabla VII-1 ilustra este tema:

Tabla VII-1

Tamaño monitor	Resolución máxima exigible (no entrelazada)	Resolución de trabajo recomendada
14"	1024x768 (monitores nuevos)	640x480
15"	1024x768	800x600
17"	1280x1024	1024x768
19"	1600x1200	1152x864
21"	1600x1200	1280x1024

Los valores recomendados para trabajar son los más cómodos, los más ergonómicos, que son los apropiados para tareas generales como las ofimáticas. Para otras más específicas como CAD, o en general cuando no nos importa forzar un poco más la vista, conviene pasar al inmediatamente superior; por ejemplo, en monitores de 19" se puede usar una resolución de 1600x1200 sin mayores problemas.

La resolución está estrechamente relacionada con el número de colores presentados, relacionado todo ello con la cantidad de memoria de la tarjeta gráfica.

Refrescamiento de pantalla

FRECUENCIA DE REFRESCAMIENTO (REFRESH RATE). Se expresa en Hz, y si esta cifra es muy baja, la imagen da una sensación de parpadeo. Para conseguir una imagen estable y sin parpadeos (FLICKER) la frecuencia de refrescamiento vertical debe ser lo mayor posible, idealmente siempre superior a 75 Hz. Los rangos normales van de 50 Hz a 160 Hz. Debemos tener mucho cuidado, pues existen en el mercado monitores que soportan 87iHz a altas resoluciones, pero la "i" pequeñita nos indica que este refrescamiento lo alcanzan en modo entrelazado, lo cual es muchísimo peor, visualmente hablando, que 60Hz.

También llamada **Frecuencia de Refrescamiento Vertical**. Se puede comparar al número de fotogramas por segundo de una película de cine, por lo que deberá ser lo mayor posible. Se mide en Hz (hertzios) y debe estar por encima de 60 Hz, preferiblemente 70 u 80. A partir de esta cifra, la imagen en la pantalla es sumamente estable, sin parpadeos apreciables, con lo que la vista sufre mucho menos.

Antiguamente los monitores sólo podían presentar imágenes con unos refrescos determinados y fijos, por ejemplo los monitores CGA o EGA y algunos VGA; hoy en día todos los monitores son multiscan, es decir, que pueden presentar varios refrescamientos dentro de un rango determinado.

Quien proporciona estos refrescamientos es la tarjeta gráfica, pero quien debe presentarlos es el monitor. **Si ponemos un refrescamiento de pantalla que el monitor no soporta podríamos dañarlo**, por lo que debemos conocer sus capacidades a fondo, para lo cual lo mejor es leer con detenimiento el manual o mirar otro parámetro denominado **Frecuencia Horizontal**, que debe ser lo mayor

Elementos de Arquitectura y Seguridad Informática

posible, entre unos 30 a 80 KHz. Por ejemplo, un monitor en que la frecuencia horizontal sea de 30 a 65 KHz dará sólo 60 Hz a 1600x1200 puntos, mientras que uno en que sea de 30 a 90 dará 75 o más.

Tamaño de punto (dot pitch).

Así se denomina a la distancia más pequeña entre 2 puntos del mismo color, se mide en centésimas de milímetros. A mayor resolución menor debe ser el dot-pitch, a menor dot-pitch más celoso será el ajuste de convergencia y más caro el monitor.

Hoy en día es difícil encontrar en el mercado un monitor nuevo con un dot pitch mayor de 0,28mm. Si el tamaño de punto es 0,27mm, 0,26mm o incluso 0,25mm (habitual en todos los monitores SONY), muchísimo mejor, pues la definición a altas resoluciones será mayor.

Es un parámetro que mide la nitidez de la imagen, midiendo la distancia entre dos puntos del mismo color; resulta fundamental a grandes resoluciones. En ocasiones es diferente en vertical que en horizontal, o se trata de un valor medio, dependiendo de la disposición particular de los puntos de color en la pantalla, así como del tipo de rejilla empleada para dirigir los haces de electrones.

Lo mínimo exigible en este momento es que sea **de 0,28 mm**, no debiéndose admitir nada superior como no sea en monitores de gran formato para presentaciones, donde la resolución no es tan importante como el tamaño de la imagen.

Para CAD o en general usos a alta resolución debe ser menor de 0,28 mm, **idealmente de 0,25 mm**. De todas formas, el mero hecho de ser inferior a 0,28 mm ya indica una gran preocupación del fabricante por la calidad del monitor. Como ejemplo cabe destacar los monitores Sony, Triniton, tienen todos un dot pitch de 0,25 mm.

Tabla VII-2. Relación dotpitch - diámetro de la pantalla.

tamaño monitor (pulgadas)	ancho imagen (mm)	dot pitch			
		640 x 480	800 x 600	1024 x 768	1280 x 1024
14	265	0.35	0.28	0.22	0.18
15	284	0.38	0.30	0.24	0.19
17	322	0.43	0.34	0.27	0.22
20	379	0.50	0.40	0.31	0.25

CONSUMO, el consumo en funcionamiento para los monitores modernos varía desde los 100 W hasta los 150 W., prácticamente todos los monitores actualmente

a la venta soportan los modos de ahorro de energía que posibilitan el paso del monitor a modo STANDBY(dormido) automáticamente tras el espacio de tiempo programado en la BIOS o en el sistema operativo.

Los DPMS (Display Power Management Signalling) sistemas de gestión de consumo de pantalla ó modos de ahorro energético suelen ser tres:

1. espera (standby),
2. reposo (suspend) y
3. apagado (off).

En cada uno de ellos el consumo es menor que en el anterior y el tiempo de recuperación mayor. No todos los monitores soportan todos los modos.

Los monitores modernos tienen implementada la circuitería de manera que permitan todos o algunos modos VGA, la polaridad de los sincronismos Horizontal y Vertical permite al circuito detector determinar en qué modo se trabaja. Por la capacidad de sincronizarse con distintas frecuencias los monitores se dividen en:

FIXED- SCAN — Trabajan a frecuencia fija (permiten variación de 5%). Estos monitores son de alta calidad y muy estables.

AUTO-SCAN — Monitores que aceptan un rango amplio continuo de frecuencias horizontal y refrescamiento vertical, permiten múltiples resoluciones y, entrada analógica o TTL, la circuitería detecta la frecuencia automáticamente y selecciona el circuito y alimentación apropiados, se acomodan a las múltiples resoluciones de diferentes programas. También son conocidos como multisync, autosync, panasync, omnisync, autoscán, mutiscán en dependencia de fabricante

La información que muestra esta tabla es proporcionada por los fabricantes de los monitores en el manual de instalación.

ENTRELAZADO- NO ENTRELAZADO, indican el modo en el que la tarjeta gráfica hace el redibujado de la pantalla.

El modo **ENTRELAZADO**, habitual en monitores antiguos y a altas resoluciones de otros monitores relativamente modernos, la tarjeta gráfica redibuja de una pasada las líneas impares y en la siguiente las líneas pares, de esta forma el cuadro de N líneas se descompone en 2 campos de N/2 líneas cada uno, con esto la pantalla se ilumina una vez con cada campo lográndose una frecuencia de refrescamiento de 50 a 60 HZ sin aumentar el ancho de banda.

Para garantizar una correcta reproducción de la imagen hay que entrelazar correctamente los campos par e impar, es decir es necesario que cada línea del segundo campo se ubique exactamente en la mitad del intervalo que existe entre 2 líneas.

Al cabo de poco tiempo puede percibirse una cierta vibración en la pantalla, con la consiguiente dificultad para leer, especialmente las fuentes de letra pequeña, y para

Elementos de Arquitectura y Seguridad Informática

observar los detalles de la imagen, por eso de ningún modo debe aceptarse una resolución habitual de trabajo en modo entrelazado.

El modo NO ENTRELAZADO consiste en redibujar todas las líneas de la pantalla en cada pasada, pero para que la imagen no muestre un leve parpadeo, este redibujado debe hacerse a una velocidad mínima de 75Hz, al menos en la resolución a la que vamos a trabajar normalmente.

MONITOR DIGITAL, el tipo de controles es lo que diferencia a los analógicos de los digitales, la mayoría usan botones para regular, sin embargo el abaratamiento de los circuitos digitales y sus facilidades para memorizar las distintas frecuencias de trabajo, resoluciones y el control digital con microprocesador los vuelven una alternativa atractiva para el diseño. Hoy los monitores de mayor calidad usan Control Digital, botones y menús en pantalla para la mayoría de los ajustes excepto posiblemente Brillo y Contraste donde el botón es más conveniente.

Un monitor digital se caracteriza por poder memorizar no sólo las frecuencias de refresco para cada resolución de acuerdo con la tarjeta gráfica, sino también los ajustes de pantalla.

Controles y conexiones

Aunque se va cada vez más al uso de monitores con controles digitales, en principio no debe ser algo determinante a la hora de elegir un monitor, si bien se tiende a que los monitores con dichos controles sean los más avanzados de la gama.

Una característica casi común a los monitores con controles digitales son los controles OSD (On Screen Control, controles en pantalla). Son esos mensajes que nos indican qué parámetro estamos cambiando y qué valor le estamos dando. Son útiles, pero en absoluto imprescindibles (ni depende la calidad del monitor de incluir dicho sistema o no).

Lo que sí suelen tener algunos monitores digitales (no todos) son memorias de los parámetros de imagen (tamaño, posición...), por lo que al cambiar de resolución no tenemos que reajustar dichos valores, lo cual puede ser bastante engorroso.

En cuanto a los controles en sí, los imprescindibles son: tamaño de la imagen (vertical y horizontal), posición de la imagen, tono y brillo. Son de agradecer los de "efecto barril" (para mantener rectos los bordes de la imagen), control trapezoidal (para mantenerla rectangular) y degauss magnético o desmagnetización.

Por lo que respecta a las conexiones, lo inexcusable es el típico conector mini D-sub de 15 pines; en monitores de 17" o más es interesante que existan además conectores BNC, que presentan la ventaja de separar los tres colores básicos. De cualquier modo, esto sólo importa si la tarjeta gráfica también los incorpora y si la precisión en la representación del color resulta determinante en el uso del monitor.

Hoy en día algunos monitores pueden incorporar una bahía USB, para la conexión de este tipo de periféricos. Resulta algo llamativo, pero para eso ya está la placa base; nunca lo tome como una auténtica ventaja.

Multimedia

Algunos monitores llevan acoplados altavoces, e incluso micrófono y/o cámaras de vídeo. Esto resulta interesante cuando se trata de un monitor de 15" ó 17" cuyo uso vaya a ser doméstico, para juegos o videoconferencia.

Sin embargo, no nos engañemos: un monitor es para ver, no para oír. Ni la calidad de sonido de dichos altavoces es la mejor posible, ni su disposición la más adecuada, ni es mayor la calidad de un monitor con dichos aditamentos. Si lo que quiere (y debería quererlo) es un buen monitor, primero mire la calidad de imagen y luego estos extras.

La elección del monitor

En líneas generales podríamos decir que existen 4 tipos principales de monitores, teniendo en cuenta que en la actualidad **los de 14" no son en absoluto recomendables para ningún uso:**

Tabla VII-3

Grupo	Tamaño	Res. recomendada	Res. máxima	Dot pitch
Económicos (ofimática, juegos)	15"	800x600 a 75 Hz	1024x768 a 60 Hz	0,28
Medios (juegos, uso general)	15"	800x600 a 80 Hz	1280x1024 a 60 Hz	0,28 a 0,25
	17"	1024x768 a 75 Hz	1280x1024 a 60 Hz	0,28
Avanzados (uso general, CAD)	17"	1152x864 a 75 Hz	1600x1200 a 60 Hz	0,27 a 0,25
Excepcionales (CAD, imágenes)	19"/21"	1280x1024 a 85 Hz	1600x1200 a 70 Hz	0,27 a 0,25

Evidentemente, aparte del uso al que va a ser destinado el monitor, el auténtico factor limitante es el propio bolsillo. No hay duda que para jugar a Quake el mejor monitor pertenecería al último grupo, si pudiéramos dejar aparte las más de 200.000 pts que costaría el capricho...

Pantallas portátiles

Se basan en tecnologías de cristal líquido (LCD) parecidas a las de los relojes de pulsera digitales pero mucho más avanzadas.

Elementos de Arquitectura y Seguridad Informática

Una de las diferencias más curiosas respecto a los monitores "clásicos" es que el tamaño que se indica es el real, no como en éstos. Mientras que en un monitor clásico de 15" de diagonal de tubo sólo un máximo de unas 13,5 a 14" son utilizables, en una pantalla portátil de 12" son totalmente útiles, así que no son tan pequeñas como parece.

Otra cosa que les diferencia es que no emiten en absoluto radiaciones electromagnéticas dañinas, por lo que la fatiga visual y los posibles problemas oculares se reducen.

En la actualidad coexisten dos tipos:

Dual Scan (DSTN): el estándar, razonablemente bueno pero que depende de las condiciones de iluminación del lugar donde se esté usando el portátil.

Matriz Activa (TFT): esta opción encarece bastante el portátil, pero permite una visualización perfecta sean cuales sean las condiciones de iluminación exteriores.

Por lo demás, en ambos casos las imágenes se ven mejor de frente que de lado, llegando a desaparecer si nos escoramos mucho, aunque en los portátiles modernos este ángulo de visión es muy alto, hasta unos 160° (el máximo es 180°, más significaría poder ver la pantalla desde la parte de atrás).

¿Qué es... una impresora?

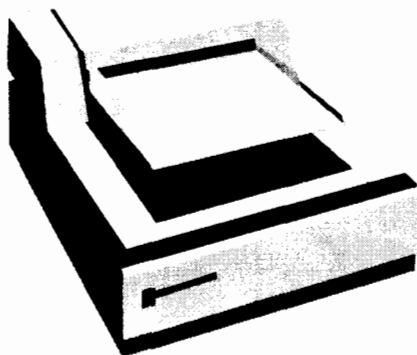


Figura VII.6 Esquema de una Impresora.

Como indica su nombre, la impresora (Figura VII.6) es el periférico que el ordenador utiliza para presentar información impresa en papel. Las primeras impresoras nacieron muchos años antes que el PC e incluso antes que los monitores, siendo durante años el método más usual para presentar los resultados de los cálculos en aquellos primitivos ordenadores, todo un avance respecto a las tarjetas y cintas perforadas que se usaban hasta entonces.

Aunque en nada se parecen las modernas impresoras a sus antepasadas

de aquellos tiempos, no hay duda de que igual que hubo impresoras antes que PCs, las habrá después de éstos, aunque se basen en tecnologías que aún no han sido siquiera inventadas. Resulta muy improbable que los seres humanos abandonemos totalmente el papel por una fría pantalla de ordenador.

Generalidades y definiciones

Antes de adentrarnos en este complejo mundo de las impresoras, vamos a exponer algunos de los conceptos básicos sobre las mismas.

Velocidad

La velocidad de una impresora se suele medir con dos parámetros:

ppm: páginas por minuto que es capaz de imprimir;

cps: caracteres (letras) por segundo que es capaz de imprimir.

Actualmente se usa casi exclusivamente el valor de ppm, mientras que el de cps se reserva para las pocas impresoras matriciales que aún se fabrican. De cualquier modo, los fabricantes siempre calculan ambos parámetros de forma totalmente engañosa; por ejemplo, cuando se dice que una impresora de tinta llega a 7 páginas por minuto no se nos advierte de que son páginas como mucho con un 5% de superficie impresa, en la calidad más baja, sin gráficos y descontando el tiempo de cálculo del ordenador.

Y aún así resulta prácticamente imposible conseguir dicha cifra; en realidad, rara vez se consiguen más de 3 ppm de texto con una impresora de tinta, si bien con una láser es más fácil acercarse a las cifras teóricas que indica el fabricante.

Resolución

Probablemente sea el parámetro que mejor define a una impresora. La resolución es la mejor o peor calidad de imagen (Figura VII.7) que se puede obtener con la impresora, medida en número de puntos individuales que es capaz de dibujar una impresora.

Se habla generalmente de **ppp**, puntos por pulgada (cuadrada) que imprime una impresora. Así, cuando hablamos de una impresora con resolución de "600x300 ppp" nos estamos refiriendo a que en cada línea horizontal de una pulgada de largo (2,54 cm) puede situar 600 puntos individuales, mientras que en vertical llega hasta los 300 puntos. Si sólo aparece una cifra ("600 ppp", por ejemplo) suele significar que la resolución horizontal es igual que la vertical.

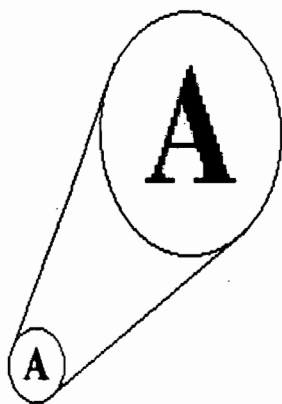
De cualquier modo, no todo es "tirar puntos" sobre el papel. Dos impresoras de la misma resolución teórica pueden dar resultados muy dispares, ya que también influye el tamaño de esos puntos y la precisión a la hora de colocarlos sobre el papel. De nada sirve colocar 360.000 puntos en una pulgada cuadrada si están puestos unos sobre otros emborronando la imagen.

El buffer de memoria

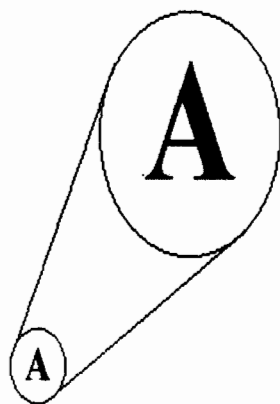
Es una pequeña cantidad de memoria que tienen todas las impresoras modernas para almacenar parte de la información que les va proporcionando el ordenador. De esta forma el ordenador, sensiblemente más rápido que la impresora, no tiene que estar esperándola continuamente y puede pasar antes a otras tareas mientras termina

Elementos de Arquitectura y Seguridad Informática

la impresora su trabajo. Evidentemente, cuanto mayor sea el buffer más rápido y cómodo será el proceso de impresión, por lo que algunas impresoras llegan a tener hasta 256 Kb de buffer (en impresoras muy profesionales, incluso varios MB).



Impresión a poca resolución



Impresión a alta resolución

Figura VII.7.

El interfaz o conector



Figura VII.8. Muestra de los conectores de una impresora.

Las impresoras se conectan al PC (Figura VII.8) casi exclusivamente mediante el **puerto paralelo**, que en muchos sistemas operativos se denomina LPT1 (LPT2 en el caso del segundo puerto paralelo, si existiera más de uno). Como el puerto paralelo original no era demasiado rápido, en la actualidad se utilizan puertos más avanzados como el ECP o el EPP, que son más rápidos y añaden bidireccionalidad a la comunicación (es decir, que la impresora puede "hablarle" al PC, lo que antiguamente era imposible) al tiempo que mantienen la compatibilidad con el antiguo estándar.

El método de trabajo del puerto paralelo (estándar, ECP, EPP...) se suele seleccionar en la BIOS del ordenador; para saber cómo hacerlo.

Físicamente, el conector para puerto paralelo presenta este aspecto en el extremo del cable que se conecta al ordenador, con 25 pines en 2 hileras, mientras que en el extremo que se conecta a la impresora suele tener 36 pines planos y unas abrazaderas. El cable para conectar ambos dispositivos se suele denominar cable paralelo Centronics; para bidireccionalidad se debe usar cables específicos, más avanzados y de mayor calidad.

Otras formas menos comunes de conectar una impresora es mediante el **puerto serie** (el que utilizan los módems externos y muchos ratones), mediante un dispositivo de **infrarrojos** (muy útil en el caso de portátiles) o directamente conectados a una **red** (y no a un ordenador conectado a la misma) en el caso de grandes impresoras para grupos.

Impresoras GDI o Win-impresoras

Antes de empezar a describir los tipos de impresoras según la tecnología de impresión que utilizan, vamos a comentar algo sobre un tipo especial de impresoras de reciente aparición en el mercado: las impresoras GDI.

GDI son las siglas de Graphical Device Interface, un tipo de tecnología propia de Windows por la cual se pueden fabricar impresoras que **cargan parte del trabajo que deberían realizar al ordenador** al que están conectadas; por ejemplo, pueden carecer de memoria propia a base de utilizar la RAM del ordenador. Gracias a este sistema se ahorran diversos componentes electrónicos en la fabricación de la impresora.

El apodo de Win-impresoras les viene dado porque el soporte para esta tarea sólo suele estar implementado para Windows (sobre todo para Windows 95), generalmente mediante un programa denominado Windows Printing System (literalmente, sistema de impresión de Windows). Puesto que Windows representa más del 90% del mercado PC, los fabricantes ni se molestan en incorporar soporte para OS/2, Linux ni otros sistemas operativos.

Las desventajas de estas impresoras son dos: primeramente, dependen de la potencia del ordenador al que están conectadas, que deberá ser como poco un Pentium rápido con una cantidad generosa de RAM; y además, **sólo funcionan en Windows**; fuera de este sistema operativo no son capaces de escribir ni una línea (ni siquiera en DOS, como no sea corriendo DOS en una ventana de Windows).

Tipos de impresoras

Si queremos clasificar los diversos tipos de impresoras que existen, el método más lógico es hacerlo atendiendo a su tecnología de impresión, es decir, al método que emplean para imprimir en el papel, e incluir en dicha clasificación como casos particulares otras consideraciones como el uso de color, su velocidad, etc. Eso nos lleva a los tres tipos clásicos: matriciales, de tinta y láser.

Impresoras de impacto (matriciales)

Fueron las primeras que surgieron en el mercado. Se las denomina "de impacto" porque imprimen mediante el impacto de unas pequeñas piezas (la matriz de impresión) sobre una cinta impregnada en tinta, la cual suele ser fuente de muchos quebraderos de cabeza si su calidad no es la que sería deseable.

Según cómo sea el cabezal de impresión, se dividen en **dos grupos** principales: de margarita y de agujas. Las **de margarita** incorporan una bola metálica en la que están en relieve las diversas letras y símbolos a imprimir; la bola pivota sobre un soporte móvil y golpea a la cinta de tinta, con lo que se imprime la letra correspondiente. El método es absolutamente el mismo que se usa en muchas máquinas de escribir eléctricas, lo único que las diferencia es la carencia de teclado.

Las impresoras de margarita y otros métodos que usan tipos fijos de letra están en completo desuso debido a que **sólo son capaces de escribir texto**; además, para cambiar de tipo o tamaño de letra deberíamos cambiar la matriz de impresión (la bola) cada vez. Por el contrario, la calidad del texto y la velocidad son muy altas, además de que permiten obtener copias múltiples en papel de autocopia o papel carbón.

Las impresoras **de agujas**, muchas veces denominadas simplemente matriciales, tienen una matriz de pequeñas agujas que impactan en el papel formando la imagen deseada; cuantas más agujas posea el cabezal de impresión mayor será la resolución, que suele estar entre 150 y 300 ppp, siendo casi imposible superar esta última cifra.

Aunque la resolución no sea muy alta es posible obtener gráficos de cierta calidad, si bien **en blanco y negro, no en color**. El uso de color implica la utilización de varias cintas o cintas más anchas, además de ser casi imposible conseguir una gama realista de colores, más allá de los más básicos.

Al ser impresoras de impacto pueden obtener copias múltiples, lo que las hace especialmente útiles en oficinas o comercios para la realización de listados, facturas, albaranes y demás documentos. Su velocidad en texto es de las más elevadas, aunque a **costa de producir un ruido ciertamente elevado**, que en ocasiones llega a ser molesto. Resulta muy común encontrarlas con alimentadores para papel continuo, lo que sólo ocurre con algunas impresoras de tinta de precio elevado.

En general, las impresoras matriciales de agujas se posicionan como impresoras de precio reducido, calidad media-baja, escaso mantenimiento y alta capacidad de impresión. Entre los pocos fabricantes de estas impresoras que quedan destaca Epson.

Impresores no matriciales

Para comenzar con la descripción de algunos tipos de impresores no matriciales, es conveniente conocer algunas características comunes a todas ellas y otras características propias a cada una.

Se puede medir la eficiencia de un impresor por la conjunción de cualidades, como por ejemplo:

- Capacidad de resolución (ppp: puntos por pulgada).
- Cantidad de hojas impresas por minuto (ppm: paginas por minuto).
- Opciones de impresión a color.
- Memoria RAM.
- Tipo de alimentación de hojas (medio).
- Como se realiza el proceso de impresión, etc.

Las características técnicas mas importantes que permiten evaluar la calidad de una impresora son:

- Velocidad de escritura: se mide en caracteres, líneas o página por segundo, según sea. Depende del mecanismo de impresión.
- Densidad de caracteres por líneas.
- Número de líneas por pulgada o por centímetro.
- Tipo de alimentación del papel: por fricción (papel en rollo para ser empujado por rodillos de goma), o por tracción (papel plegado con perforaciones laterales, para dientes de arrastre).
- Ancho del papel que se puede utilizar.
- Posibilidad de escribir distintos tipos de letras y caracteres especiales.
- Numero máximo de copias.
- Capacidad de graficación.
- Normas utilizadas para conexionado: las mas corrientes son RS 232 (transmisión en Serie), IEEE 488 y Centronics (transmisión paralela).

Impresoras sin impacto

- 1.- Térmicas
- 2.- Electrostáticas
- 3.- Por chorro de tinta
- 4.- Láser

Impresoras térmicas

Una cabeza móvil presenta una matriz de puntos, que pueden calentarse por la acción de resistores. Los puntos calientes forman el carácter a imprimir, y al ser aproximados al papel termosensible, lo imprimen por calor, resultando una formación de puntos más oscuros. El resultado es semejante al de la figura 9.26. El controlador determina qué resistores se calentarán, ordenando la circulación de corrientes eléctricas por los mismos. Se trata de una impresión por formaciones de puntos, como en la impresora de matriz de agujas, pero al no percutir la matriz sobre el papel resulta un funcionamiento totalmente silencioso. Y por no existir vibraciones mecánicas se simplifica el diseño del sistema resultando económico, aunque por otra parte el costo del papel termosensible es relativamente elevado.

La calidad de la impresión está determinada por la densidad de los puntos la que será limitada horizontalmente por la velocidad de barrido de la cabeza y verticalmente por el tamaño del resistor. La disminución del consumo posibilita versiones portátiles con baterías.

Estas impresoras tienen una velocidad de impresión comparable a las impresoras de caracteres más lentas.

Impresoras electrostáticas

Consisten en un tambor cilíndrico, con superficies de selenio, donde la carga eléctrica de las mismas está controlada por la intensidad de un haz de luz incidente. Dicho haz, modulado por la señal recibida por el controlador, realiza un barrido del área del tambor. La distribución de cargas sobre cada superficie será entonces proporcional a la intensidad del haz modulado. Los distintos puntos, cargados eléctricamente, atraerán el tonner, cargado en forma similar al de una fotocopiadora. El Tambor transfiere luego el tonner al papel, para reproducir la imagen a través de la aplicación de presión y calor. Graduando el voltaje aplicado se pueden obtener desde puntos finos y brillantes hasta puntos más opacos, lográndose muy buenos grisados. La calidad de impresión de las copias depende, en gran medida, del papel. Se pueden lograr velocidades del orden de centenares de páginas por minuto.

Impresoras de tinta

Por supuesto, las impresoras matriciales son impresoras de tinta, pero cuando nos referimos a impresora de tinta nos solemos referir a aquellas en las que la tinta se encuentra en forma más o menos líquida, no impregnando una cinta como en las matriciales.

La tinta suele ser impulsada hacia el papel por unos mecanismos que se denominan inyectoros, mediante la aplicación de una carga eléctrica a un cristal piezoeléctrico,

que envía la señal de sincronización, siendo las gotitas equidistantes entre sí, lo que hace saltar una minúscula gota de tinta por cada inyector, sin necesidad de impacto. La dirección de las gotas se logra en forma electrostática por medio de los electrodos que actúan como placas de deflexión de las gotas cargadas eléctricamente. De este modo la disgregación del chorro en gotas forma los puntos de un carácter a imprimir en el papel, situado delante del cabezal. De todas formas, los entresijos últimos de este proceso varían de una a otra marca de impresoras (por ejemplo, Canon emplea en exclusiva lo que denomina "inyección por burbuja") y no son realmente significativos a la hora de adquirir una u otra impresora. Estas impresoras permiten velocidades de 150 cps.

Estas impresoras destacan por la sencilla **utilización del color**. Antiguamente (y todavía en algunos modelos de muy baja gama o en impresoras portátiles), para escribir cualquier cosa en color se tenía que sustituir el cartucho de tinta negra por otro con tintas de los colores básicos (generalmente magenta, cyan y amarillo). Este método tenía el inconveniente de que el texto negro se fabricaba mezclando los tres colores básicos, lo que era más lento, más caro en tinta y dejaba un negro con un cierto matiz verdoso. En la actualidad, la práctica totalidad de estas impresoras incorporan soporte para el uso simultáneo de los cartuchos de negro y de color.

La resolución de estas impresoras es en teoría bastante elevada, hasta de 1.440 ppp, pero en realidad la colocación de los puntos de tinta sobre el papel resulta bastante deficiente, por lo que no es raro encontrar que el resultado de una impresora láser de 300 ppp sea mucho mejor que el de una de tinta del doble de resolución. Por otra parte, suelen existir papeles especiales, mucho más caros que los clásicos folios de papelería, para alcanzar resultados óptimos a la máxima resolución o una gama de colores más viva y realista.

El principal destinatario de este tipo de impresoras es el usuario doméstico, además del oficinista que no necesita trabajar con papel continuo ni con copias múltiples pero sí ocasionalmente con color (logotipos, gráficos, pequeñas imágenes...) con una calidad aceptable. Fabricantes existen decenas, desde los clásicos contendientes Epson y Hewlett-Packard (hp) hasta otros de mucho menor volumen de ventas pero que no desmerecen nada, como son Canon, Tektronik, Lexmark, Oki...

Una nota sobre los cartuchos de tinta: son relativamente caros, debido a que generalmente no sólo contienen la tinta, sino parte o la totalidad del cabezal de impresión; este sistema asegura que el cabezal siempre está en buen estado. Existen decenas de sistemas de recarga de cartuchos para rellenar el cartucho aprovechando el cabezal, pero en el 99% de los casos son un engorro y se pone todo perdido de tinta; no se los recomiendo para nada.

Impresoras láser

Son las de mayor calidad del mercado, si entendemos por calidad la resolución sobre papel normal que se puede obtener, **unos 600 ppp reales**. En ellas la impresión se consigue mediante un láser (Figura VII.9) que va dibujando la imagen electrostáticamente en un elemento llamado tambor que va girando hasta

Elementos de Arquitectura y Seguridad Informática

impregnarse de un polvo muy fino llamado tóner (como el de fotocopiadoras) que se le adhiere debido a la carga eléctrica. Por último, el tambor sigue girando y se encuentra con la hoja, en la cual imprime el tóner que formará la imagen definitiva.

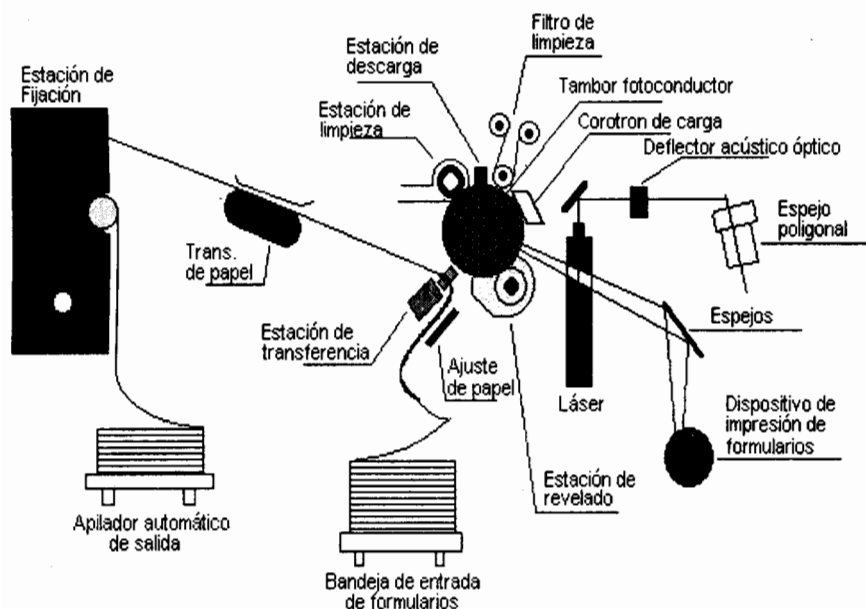


Figura VII.9. Esquema que muestra el principio de funcionamiento de una impresora Láser

Las peculiares características de estas impresoras obligan a que dispongan de su propia memoria para almacenar una copia electrónica de la imagen que deben imprimir. A mayor tamaño y calidad de impresión necesitaremos mayor cantidad de memoria, que estará entorno a 1 ó 2 MB; si el documento a imprimir fuera muy largo y complejo, por ejemplo con varias fotografías o a una resolución muy alta, puede producirse un error por overflow (falta de memoria), lo que puede evitarse mediante la tecnología GDI comentada anteriormente o preferiblemente instalando más memoria a la impresora.

El único problema de importancia de las impresoras láser es que **sólo imprimen en blanco y negro**. En realidad, sí existen impresoras láser de color, que dan unos resultados bastante buenos. Sin embargo, las láser son muy resistentes, mucho más rápidas y mucho más silenciosas que las impresoras matriciales o de tinta, y aunque la inversión inicial en una láser es mayor que en una de las otras, el tóner sale más barato a la larga que los cartuchos de tinta, por lo que a la larga se recupera la inversión. Por todo ello, las láser son idóneas para entornos de oficina con una intensa actividad de impresión, donde son más importantes la velocidad, la calidad y el escaso coste de mantenimiento que el color o la inversión inicial.

Dada la gran capacidad de impresión de éstas, son elegidas por la mayoría de las empresas que trabajan en redes de información (Figura VII.10), con un gran volumen de impresión.

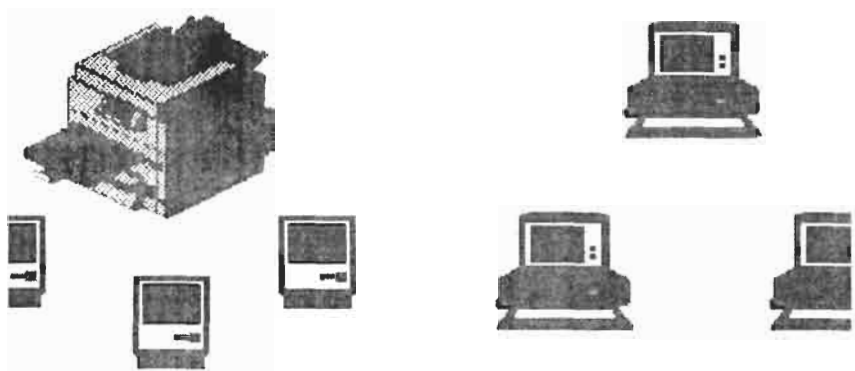


Figura VII.10. Esquema que muestra la forma de trabajar las impresoras en red.

Otros tipos de impresoras

Vamos a tratar ahora de otras impresoras de uso mucho menos común, pero que cubren ciertas necesidades concretas del mercado, como pueda ser los grandes formatos o la calidad fotográfica.

Plotters

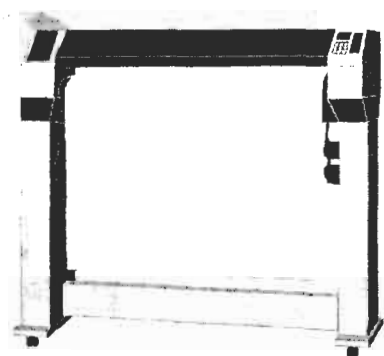


Figura VII.11 Plotters.

Se trata de unos aparatos destinados a la impresión de planos para proyectos de arquitectura o ingeniería, (Figura VII.11) por lo que trabajan con enormes formatos, DIN-A1 (59,4x84 cm) o superiores. Antiguamente consistían en una serie de plumillas móviles de diferentes grosores y colores que se movían por la hoja reproduciendo el plano en cuestión, lo que era bastante incómodo por el mantenimiento de las plumillas y podía ser impreciso al dibujar elementos tales como grandes círculos.

En la actualidad casi todos tienen mecanismos de inyección de tinta, facilitando mucho el mantenimiento, que se reduce a cambiar los cartuchos; son auténticas impresoras de tinta, sólo que el papel es mucho más ancho y suele venir en rollos de decenas de metros.

Impresoras para fotos

Constituyen una categoría de reciente aparición; usan métodos avanzados como la **sublimación** o las ceras o tintas sólidas, que garantizan una pureza de color excepcional, si bien con un coste relativamente elevado en cuanto a consumibles y una velocidad baja.

La calidad de estas impresoras suele ser tal, que muchas veces el resultado es indistinguible de una copia fotográfica tradicional, incluso usando resoluciones relativamente bajas como 200 ppp.

Sin embargo, son más bien caras y los formatos de impresión no suelen exceder el clásico 10x15 cm, ya que cuando lo hacen los precios suben vertiginosamente y nos encontramos ante impresoras más apropiadas para pruebas de imprenta y autoedición.

Impresoras de gran formato

Resulta una frase tan buena como cualquier otra para definir a las impresoras, casi exclusivamente de tinta, que imprimen en formatos hasta el A2 (42x59,4 cm). Son impresoras que reúnen las ventajas de las impresoras de tinta en cuanto a velocidad, color y resolución aceptables junto a un precio bastante ajustado, menos de 150.000 pts, lo que es una pequeña fracción del precio de un plotter.

Se utilizan para realizar carteles o pósters, pequeños planos o pruebas de planos grandes, así como cualquier tarea para la que sea apropiada una impresora de tinta de menor formato: cartas, informes, gráficos... Hasta hace poco sólo existían un par de modelos, ahora las hay de Epson, Canon e incluso HP.

Impresoras para grupos

Son impresoras de gran capacidad, preparadas para funcionar en una red incluso sin depender de un ordenador de la misma. Suelen ser impresoras láser, en ocasiones con soporte para color, con bandejas para 500 hojas o más, velocidades de más de 12 ppm (reales!!) y memoria por encima de 6 MB. Últimamente se tiende a que tengan funciones de fotocopidora o capacidad para realizar pequeñas tiradas sin necesidad de emplear una fotocopidora, e incluso clasifican y encuadernan.

Adecuación al uso

Realmente está todo dicho ya en los apartados anteriores; sin embargo, vamos a resumirlo aquí para aclarar un poco las cosas:

Tabla VII-4

Uso	Impresora a utilizar	Comentarios
Textos, copias múltiples, listados, facturas	Matricial	Baratas, bajo mantenimiento, poca resolución
Textos y gráficos en blanco y negro y color	De tinta	Baratas, consumibles algo caros, resolución aceptable
	Láser color	Caras, muy rápidas, alta resolución; para grandes cargas de trabajo
Textos y gráficos en blanco y negro	Láser blanco y negro	Mayor inversión inicial, menor mantenimiento, alta resolución
Formatos grandes, posters, carteles, planos	De tinta gran formato	Baratas, formatos algo reducidos para planos (A3, A2)
	Plotter	Caros, específicos para planos, formatos A1 o A0
Fotografías	Sublimación, ceras sólidas o similar	Caras en consumibles, formato reducido, algo lentas, gran calidad, muy caras en formatos grandes
Grandes cargas de trabajo	Láser color o blanco y negro de alta gama	Caras, bajo mantenimiento, alta velocidad y resolución

VIII. Seguridad informática

Seguridad de la Información.

Dando por bueno que la seguridad trata de la protección de los bienes, parece natural establecer cuáles son los bienes informáticos a proteger. En una primera panorámica podríamos decir que éstos son: el hardware; el software y los datos. De estos bienes, los más expuestos a todo tipo de riesgos, y también los que más rápidamente se devalúan, son los datos. Están expuestos a más riesgos, puesto que son accedidos por más personas: usuarios; analistas; programadores, que los restantes bienes y sometidos a las mismas amenazas no intencionadas que los demás. Son los que más rápidamente se devalúan, pues su tiempo de vida útil suele ser corto y pierden su valor más rápidamente que el hardware, cuyo tiempo de vida útil se suele estimar en torno a 2 o 3 años y el software que en algunos casos (p. ej., los de gestión y control) con los mantenimientos oportunos, se mantiene operativo durante más de 5 años.

Naturalmente podríamos listar otros bienes a proteger como: personal informático; materiales fungibles; suministros de potencia y aire acondicionado; sistemas de transmisión de datos; etc., pero, por un lado, son bienes no intrínsecamente informáticos (aunque imprescindibles para el desarrollo de la función informática) y, por otro, su protección viene dada por los mismos mecanismos que los de los tres bienes enunciados anteriormente.

Las amenazas que se ciernen sobre los sistemas informáticos tienen orígenes diversos. Así, si consideramos las amenazas externas, el hardware puede ser físicamente dañado por agua, fuego, sabotajes, y otros. Las mismas causas pueden dañar los medios magnéticos de almacenamiento externo. La información contenida en éstos, también puede verse afectada por campos magnéticos intensos y, frecuentemente, por errores de operación. Las líneas de comunicación pueden ser interferidas o "pinchadas", etc.

Otros tipos de amenazas provienen de usuarios o empleados infieles. Así, los primeros pueden usurpar la personalidad de usuarios autorizados y acceder indebidamente a datos para su consulta o borrado, o, aunque algo más complicado, modificar en su provecho programas de aplicación.

Otras amenazas más sutiles provienen de inadecuados controles de programación. Así, el problema de residuos, es decir, de la permanencia de información en memoria principal cuando ésta es liberada por un usuario o, en el caso de dispositivos externos cuando ésta es incorrectamente borrada. Una técnica fraudulenta muy usada consiste en transferir información de un programa a otro mediante canales ilícitos y no convencionales (canales ocultos).

El comportamiento de las amenazas a la seguridad de la información arroja que la mayoría de los hechos son realizados por intrusos individuales. Un por ciento menor corresponde a incidentes realizados por grupos organizados, otro por ciento aun menor son delitos y la punta de la pirámide corresponde a casos de espionaje, (industrial, económico, militar...). Según la Oficina de Ciencia y Tecnología de la Casa Blanca las pérdidas anuales estimadas en USA por espionaje económico ascienden a \$ 100 Miles de Millones de USD.

Las principales amenazas de Internet son:

- Los ANEXOS a mensajes enviados por email infectados por virus.
- El intercambio de códigos de virus.
- Los FIREWALLS o Cortafuegos mal configurados.
- Los ataques a la disponibilidad de Recursos.
- Alteración de páginas Web.
- El "Repudio" y las estafas asociado al Comercio Electrónico.
- Las vulnerabilidades de los Sistemas Operativos y la no actualización de los PARCHES concernientes a la Seguridad de los mismos.
- La rotura de contraseñas.
- La suplantación de identidad
- El acceso a páginas pornográficas, terroristas, etc.
- El robo y la destrucción de información
- Pérdida de tiempo durante el acceso a sitios ajenos a la razón social de la entidad.
- El hecho de que herramientas de Hacking y Cracking se ofrecen como FREEWARE

Seguridad física y lógica

El término seguridad física es el usualmente empleado para describir las medidas de protección externas adora, que tratan de proteger a éste y su entorno de amenazas físicas. Normalmente, se materializan mediante dispositivos eléctricos, electrónicos, etc.

De todas las medidas de protección ya esbozadas las físicas son, probablemente, las primeras que en todas las instalaciones informáticas se adoptan. Ello es debido a dos factores; por un lado, aunque la probabilidad de que se produzca un incendio o una inundación sean mucho menor que las probabilidades de ocurrencia de otras amenazas, ante una catástrofe como las citadas las pérdidas serían completas.

Elementos de Arquitectura y Seguridad Informática

Por otro lado, estas medidas de protección son usualmente las más fáciles de tomar. Su costo no es excesivo (con la excepción de los sistemas de continuidad eléctrica) y su mantenimiento no ofrece especiales problemas.

Una primera medida de protección para las salas de Centros de Proceso de Datos (CPD), común a todas las amenazas expuestas es la ubicación geográfica adecuada de las mismas. Una segunda consideración, también general, es la correcta construcción de dicha sala y su situación idónea dentro del edificio.

Las siguientes medidas son ya específicas para cada tipo de amenaza, por lo que las expondremos bajo el riesgo que contribuyen a prevenir.

- **Inundaciones (intensas lluvias, desborde de ríos, penetraciones del mar, etc.)**

La mejor medida es la adecuada ubicación de los equipos, en edificios alejados de zonas potencialmente peligrosas (cercañas de barrancos y cauces de ríos, zonas bajas de la costa, etc.). En todo caso estos sistemas conviene situarlos en plantas altas.

- **Inundaciones internas**

Además de las medidas constructivas (no deben pasar conducciones de agua por los techos ni paredes, debe haber desagües en el piso real, el cual debe presentar una inclinación hacia estos, etc.) existen detectores de humedad, que situados en el piso real podrían avisar de la inundación. Además, se recomienda tapar con forros plásticos los equipos cuando no se usen (sobre todo los PC's).

- **Fuegos**

Los sistemas de detección/extinción de incendios son de sobra conocidos. En la actualidad, el elemento extintor más usado es el halón, gas anticatalítico de la reacción química que produce el fuego y que en pequeña proporción no es inmediatamente tóxico.

Actualmente se investigan a marchas forzadas sustitutos, pues por el daño elevadísimo que producen a la capa de ozono, se acordó en la Convención de Montreal su total eliminación.

- **Caídas de tensión**

En este epígrafe se consideran tanto las caídas propiamente dichas (cortes de más de pocos milisegundos), microcortes, transitorios, etc. Lo más eficaz contra estas anomalías del suministro es un sistema de alimentación ininterrumpida (SAI o UPS en inglés) en línea (los fuera de línea precisan de unos microsegundos, tiempo de conmutación, para actuar). De ser los tiempos prolongados se necesitaría un equipo electrógeno de respaldo.

- **Calor**

La protección pasa por la instalación de alarmas que se disparan caso de subir o bajar la temperatura de la sala por encima o debajo de los límites permitidos.

- **Interferencias electromagnéticas**

La solución óptima es el apantallamiento de la sala de ordenadores y en el caso de terminales el uso de aquéllos con certificación TEMPEST (enmascaramiento de pulsos electromagnéticos transientes). Para las líneas de comunicación (las más expuestas) el uso exclusivo de las apantalladas o, más seguro todavía, fibra óptica.

- **Atentados**

Su prevención se consigue mediante estrictos controles de acceso a las áreas del ordenador y su entorno. En el caso de costosas o críticas instalaciones, los sistemas biométricos (mejor se debería decir bioantropométricos) son de gran fiabilidad. Entre estos se deben citar: reconocimiento de las huellas digitales, del patrón de las venas del fondo de ojo, de la forma de la mano, de la voz, etc. Además, se pueden instalar equipos de reconocimiento de materiales que entran en las instalaciones.

- **Hurtos**

El problema actual más grave lo constituyen los ordenadores personales y sus partes componentes, cuya fácil portabilidad presenta un gran riesgo. Existen ya sistemas de anclaje muy efectivos y otros, que en conjunción con arcos en las salidas, permiten prevenir esta amenaza.

Medidas de seguridad técnicas o lógicas

Por lo que respecta a las medidas técnicas pretenden proteger tanto el software, sea de base o de aplicación, como los datos. Estas medidas pueden implementarse en dispositivos hardware o en productos software.

Para el desarrollo de estas medidas, se ha hecho necesaria una investigación académica muy intensa, principalmente en la última década y media, que ha dado lugar a modelos teóricos del máximo interés como pueden ser: modelos de control de accesos; modelos de control de flujo de información; desarrollo de criptosistemas de clave privada y pública; desarrollo de sistemas de firma digital y no-repudio en transmisión de datos.

A continuación expondremos muy someramente los temas más notables de estas medidas de protección.

- **Criptografía.**

A diferencia de las otras ramas del conocimiento que fundamentan la informática, todas ellas muy jóvenes, la criptografía (y por tanto la criptología) hunde sus orígenes, al menos, en la antigüedad clásica. Así, el escitalo lacedemonio era un instrumento criptográfico (un simple bastón con una tira de papel enrollado) ya usado durante las guerras entre espartanos y atenienses, y el cifrado CESAR, empleado aún hoy en día para ejemplarizar los métodos criptográficos de sustitución, fue ideado por los romanos.

Por contra de los ejemplos anteriores, los métodos criptográficos son usados actualmente no sólo en temas relacionados con la guerra o el espionaje, sino que la

Elementos de Arquitectura y Seguridad Informática

sociedad de la información en la que vivimos, precisa de medios seguros de transportar y almacenar todo tipo de información, sea comercial, sanitaria, estadística o de cualquier otra clase, y así la criptografía ha experimentado en los últimos tiempos un fuerte desarrollo, que ha originado la aparición continua de nuevos y complejos algoritmos criptográficos, cuyos dos principales paradigmas son el RSA y el DES.

La palabra criptología deriva del griego Kriptos, oculto, y abarca tanto la criptografía, o sea, la protección de la información a través de su codificación mediante claves, como el criptoanálisis, es decir, la supresión de esa protección sin el conocimiento de la clave.

La criptografía asume generalmente que el criptoanalista tiene pleno acceso al criptograma. Así mismo, se acepta el principio enunciado por Dutchman A. Kerckhoff: "La seguridad del cifrado debe residir exclusivamente en el secreto de la clave". En otras palabras, el Principio de Kerckhoff establece que todo el mecanismo del cifrado, excepto el valor de la clave, es conocido por el criptoanalista.

Frecuentemente, los criptosistemas utilizan la misma clave para cifrar y para descifrar (o, si son distintas, del conocimiento de una se deduce la otra), son los criptosistemas de clave única o simétricos.

Por contra, otros métodos criptográficos usan dos claves distintas (no pudiéndose obtener a no ser que se posea una información adicional) para las operaciones citadas, denominándose criptosistemas de dos claves o asimétricos.

• Sistemas operativos

El principal problema en la construcción de sistemas informáticos seguros, es el diseño, desarrollo e implementación de sistemas operativos que satisfagan estrictas políticas de seguridad.

Para que un sistema operativo sea seguro debe ser diseñado de modo que: identifique y autentique a todos los usuarios, controle el acceso a todos los recursos e informaciones, contabilice todas las acciones realizadas por usuarios (o procesos invocados por ellos), audite los acontecimientos que puedan representar amenazas a la seguridad, garantice la integridad de los datos, mantenga la disponibilidad de recursos e informaciones, etc. Todos estos aspectos han venido siendo estudiados con interés creciente en las dos últimas décadas, creándose modelos teóricos de gran importancia, que recientemente se han empezado a implementar en sistemas operativos comerciales.

Históricamente los primeros mecanismos de seguridad que se introdujeron en los sistemas operativos fueron la identificación y autenticación, esta última mediante contraseñas sólo conocidas por el usuario. Aunque este sistema sigue siendo el mayoritariamente usado, han empezado a aparecer otras formas de autenticación, entre ellas:

Identificación por hardware: el usuario o el terminal al que está conectado, posee un dispositivo hardware que identifica inequívocamente al mismo;

Características bioantropométricas del usuario, como pueden ser: huellas digitales; patrones de voz; imagen de la palma de la mano; mapa de las venas del fondo del ojo; etc.;

Conocimientos, aptitudes, hábitos del usuario; por ejemplo: características dinámicas de la firma (tiempo, aceleraciones, inclinaciones); estilo de pulsación del teclado; rasgos del uso del ratón; etc;

Información predefinida que posee el usuario: datos personales; culturales; aficiones; frases-contraseña; etc.;

Además, el modelo simple de contraseñas se ha venido perfeccionando, para evitar los riesgos que conlleva la utilización repetida de los mismos caracteres para acceder al sistema. Así, han aparecido los modelos de contraseña variable; de lista de contraseñas; basados en funciones unidireccionales; los generadores de contraseñas, y otros muchos que aunque todavía no generalizados son usados en ciertas aplicaciones con estrictos requisitos de seguridad.

Mención aparte merece el cifrado de contraseñas, cada vez más usado para evitar que los ataques a la tabla de contraseñas del sistema puedan revelar las mismas.

• **Redes de ordenadores**

Por la aceptación que están obteniendo los estándares de la Organización Internacional de Estándares (ISO) sobre los "Open Systems Interconnection", y por la creciente influencia que ejercen, vamos a exponer la **arquitectura de seguridad** de dichas normas que, además, ejemplifica muy bien los **conceptos básicos sobre los que se asientan todas las arquitecturas de seguridad.**

En la arquitectura citada, hay cuatro capas de la torre de niveles OSI donde se pueden implementar los mecanismos de **seguridad pertinentes.** La implantación en uno u otro nivel dependerá de los **requisitos de seguridad a satisfacer, que pueden clasificarse también en cuatro divisiones.**

Así, un dispositivo de cifrado a nivel físico o a nivel de enlace es la solución si se desea conectar redes seguras, pero mediante enlaces inseguros. En efecto, aunque las redes de origen y de destino sean seguras, si el camino entre los nodos atraviesa alguna red insegura (por ejemplo, una red pública de datos), se precisa añadir mecanismos de seguridad en el nivel de transporte.

Sin embargo, si los ordenadores que desean comunicarse no tienen la certeza de que las redes a las que pertenecen sean seguras, se precisa que la seguridad se extienda extremo a extremo. Este tipo de seguridad se puede implementar en el nivel de red o de transporte. Ambas opciones están en consideración en los comités de normalización correspondientes.

Elementos de Arquitectura y Seguridad Informática

Finalmente, algunos usuarios que sólo desean proteger algunas aplicaciones, o algunos campos de ciertas aplicaciones, necesitan implementar la seguridad en el nivel de aplicación, aunque a veces también se procede en el nivel presentación.

Los tres conceptos básicos de la arquitectura de seguridad de OSI son: amenazas a la seguridad, servicios de seguridad y mecanismos de seguridad.

Las primeras son acciones potenciales que pueden comprometer la seguridad de la información.

Se pueden clasificar en pasivas y activas.

Las amenazas pasivas consisten en el registro o detección de los datos mientras son transmitidos. Por no suponer alteración de los mismos son difíciles de detectar y de imposible recuperación, por lo que el único tipo de medidas de protección lo constituyen las preventivas. Las dos modalidades de estas amenazas son la lectura de datos y el análisis del tráfico. En este último caso el atacante se limita a leer las cabeceras de los paquetes, donde puede encontrar la identidad y situación de los nodos. También puede, a partir de aquí, obtener la frecuencia de los mensajes entre dos nodos lo que constituye, en ocasiones, una valiosa información.

Las amenazas activas se materializan mediante la conexión de un dispositivo a la línea de transmisión para alterar o borrar señales o generar otras nuevas. Pueden consistir en: la destrucción (o retraso) de todos los mensajes que circulan por una línea, la modificación del flujo de mensajes, sea borrando alterando, retrasando o reordenando algunos mensajes.

Por otra parte, un mecanismo de seguridad es una implementación hardware o software diseñada y construida para prevenir, detectar o recuperarse de la materialización de una amenaza. Cada servicio de seguridad es implementado mediante uno o varios mecanismos de seguridad.

Los mecanismos considerados en la norma OSI citada son: cifrado, firma digital, control de accesos, integridad de los datos, intercambio de autenticación, rellenado de tráfico, control de rutas y notarización.

Finalmente, las normas OSI definen un servicio de seguridad como una función suministrada por un sistema de comunicación para mejorar su seguridad. Los servicios definidos son: confidencialidad, integridad, autenticidad, control de accesos y no repudio.

El uso de sistemas de interconexión abiertos (OSI), muy recomendable por su versatilidad y por su rápida implantación, incrementa las amenazas a la información con lo que el mantenimiento de la confidencialidad, integridad y disponibilidad es una tarea mucho más ardua.

● Evaluación y certificación de la seguridad

Finalmente, cabe resaltar que a la par que el interés se ha desplazado hacia estas medidas técnicas, se ha ido poniendo de manifiesto la necesidad de evaluar la

calidad de las funciones de seguridad que los sistemas de información iban incorporando. Desgraciadamente, esta evaluación no puede realizarse mediante una métrica exacta; por lo que la verificación de estas funciones de seguridad debe hacerlas una institución neutral y digna de confianza. Además, el proceso de verificación debe ser transparente, lo que es sólo posible mediante una descripción detallada de los procesos que se han seguido y los correspondientes criterios de verificación.

Plan de seguridad informática

El Plan de Seguridad Informática constituye el documento básico para lograr la confidencialidad, integridad y disponibilidad de la información y la protección de los medios y los locales donde se utilice la técnica de computación.

En el desarrollo de este plan es necesario formular la política de seguridad, establecer una estructura de gestión de la seguridad informática, elaborar el sistema de medidas de seguridad informática, implantar el programa de seguridad informática y elaborar el plan de contingencia de la entidad.

Previo a la formulación de la política de seguridad, se deben considerar diferentes aspectos referentes a la información en la organización. Así, es imprescindible hacer un estudio de:

1. grado de criticidad de los diversos servicios respecto de la información y del valor de ésta para aquellos;
2. nivel de inversión en Tecnologías de la Información;
3. amenazas (sean accidentales o intencionadas) que sufre la información;
4. las vulnerabilidades de los sistemas y productos de T.I. existentes;
5. las medidas de seguridad ya implantadas.

Con este estudio previo se puede ya elaborar la política de seguridad. Ésta es el conjunto de principios y reglas generales que regulan la forma, propia de cada organización, de proteger las informaciones que maneja en todas las fases de su tratamiento.

Un factor determinante en la elaboración de esta política, y consecuentemente en el éxito del plan de seguridad, es la implicación de los máximos responsables de la institución. A no ser que éstos comprendan y se involucren en los objetivos de la política de seguridad su final feliz será incierto. La veracidad de esta afirmación resulta de considerar que la política de seguridad afecta a todos los servicios y niveles dentro de éstos, así como a los flujos de información entre diferentes servicios, de éstos al exterior y viceversa. Es decir, involucra a todo el sistema de información de la organización.

• POLÍTICA DE SEGURIDAD INFORMÁTICA

La política de seguridad que nos ocupa puede contener principios específicos para algunos servicios en los que la seguridad de la información sea especialmente

Elementos de Arquitectura y Seguridad Informática

crítica. O también, puede incluir aspectos convenientes sólo a ciertos equipos, como pueden ser ordenadores personales.

Entrando ya en los contenidos de la política de seguridad, ésta debe comenzar postulando que la información es un activo más del organismo y cuáles son las características a priorizar de este activo: la confidencialidad (impedir la divulgación no autorizada); la integridad (impedir la modificación no autorizada) y la disponibilidad (impedir la retención no autorizada). Se deben tratar, al menos, los siguientes aspectos:

Organizativos:

Se deben definir las responsabilidades de los empleados, y el papel que desempeñan éstos, en la protección de la información y las líneas de dependencia funcionales a este respecto. Igualmente, se debe crear una estructura departamental específica, responsable de coordinar y controlar en todo el organismo la seguridad de la información.

De Personal:

Se deben contemplar aquí, sobre todo, los aspectos de concienciación y formación en seguridad.

Igualmente, se deben tratar los aspectos sancionadores, caso de incurrir en negligencias, las políticas de contratación y el empleo de personal externo cuando sea preciso. Todo ello bajo la perspectiva de la seguridad.

De Procedimiento:

La política de seguridad se debe considerar como una referencia obligada en todo el ciclo de vida de los sistemas de información. Así, la seguridad de las T.I. debe ser tenida en cuenta en el desarrollo de todas las aplicaciones (estableciendo el modo de hacer esto), en la adquisición de equipos físicos y lógicos (incluyendo cláusulas específicas en los contratos), en la instalación y mantenimiento de éstos, etc.

Así mismo, se debe definir la manera de mantener y cambiar, en su caso, estos procedimientos.

Clasificación de la información:

La información debe ser clasificada de acuerdo con su sensibilidad e importancia para la organización, ya que no es posible esperar que los directivos y trabajadores mantengan un absoluto control sobre toda la información que manejan; así pues, es necesario que conozcan: primero, qué informaciones son consideradas más sensibles y, segundo, cómo se deben manejar y proteger estas informaciones.

La implantación de esta clasificación suele encontrar resistencia en el personal, que acusa el incremento de trabajo que supone. Es por tanto imprescindible una operación de "venta" a los empleados de este sistema; así como limitar al máximo las informaciones tipificadas en el más alto nivel.

Así mismo, se considerará la manera de desclasificar, etiquetar, almacenar, acceder, destruir y reproducir las informaciones según dicho nivel de clasificación.

Manejo de incidentes:

Se establecerá un registro de incidentes de la seguridad de la información, que capacite a los departamentos para analizar las tendencias, prever incidentes futuros y concentrar los recursos de seguridad de la manera más eficiente.

Análisis de riesgos:

Se especificará el método para analizar los riesgos de la información, así como para definir riesgos máximos asumibles.

Auditoría:

Se establecerá la extensión y periodicidad de las auditorías de seguridad internas y externas. En los reportes finales de las auditorías deberá siempre establecerse la elaboración de un Plan de Medidas para la solución de los problemas encontrados. Según la extensión y ambición con que se aborde la política de seguridad, se pueden afrontar más o menos temas, aunque los anteriores deberían considerarse los mínimos a contemplar.

• ESTRUCTURA DE GESTION

Por lo que respecta a la determinación de la estructura de gestión, debe crearse una unidad (departamento, sección, grupo, etc.) específica encargada de **gestionar** la seguridad.

Sistema de medidas de seguridad

Se relacionarán las medidas necesarias para **garantizar la seguridad de la información** a partir de los objetivos planteados.

Las medidas que se definirán en el documento se clasificarán según su función, las cuales pueden ser de; Seguridad Física, Seguridad Técnica o Lógica, Administrativas u Organizativas, Seguridad de Operaciones, Legales y Educativas o de Concientización. Según su forma de actuar dentro del sistema de la Entidad y las mismas pueden ser de tipo preventivas, detectivas o correctivas, y partiendo de estas clasificaciones se ordenarán las medidas.

Plan de contingencia

Se denomina Plan de Contingencia (también de recuperación de desastres o de continuación de negocios), a la definición de acciones a realizar, recursos a utilizar y personal a emplear caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización. Es decir, es la determinación precisa del quién, qué, cómo, cuándo y dónde, caso de producirse una anomalía en el sistema de información.

Elementos de Arquitectura y Seguridad Informática

El Plan de Contingencia debe considerar todos los componentes del sistema: Datos críticos, equipo lógico de base, aplicaciones, equipos físicos y de comunicaciones, documentación y personal. Además, debe contemplar también todos los recursos auxiliares, sin los cuales el funcionamiento de los sistemas podría verse seriamente comprometido: suministro de potencia; sistemas de climatización; instalaciones; etc. Finalmente, debe prever también la carencia, por cualquier motivo, de personal calificado para el correcto funcionamiento del sistema.

Se debe destacar, que previo al comienzo del trabajo, se debe obtener el pleno compromiso de los máximos responsables de la organización. Sin su apoyo el fracaso del plan está garantizado.

Programa de seguridad

El programa de seguridad deberá desarrollar la política de seguridad y luego implementar y mantener este desarrollo. Se deberán identificar proyectos y productos, establecer calendarios, asignar prioridades, acordar recursos, y fundamentalmente, dictar procedimientos concretos. Estos procedimientos serán administrativos, técnicos, físicos y de personal. Entre los primeros: clasificación de la información; privilegios de acceso; gestión de la configuración; registro de incidencias; uso de programas externos; control y etiquetado de documentos; almacenamiento y destrucción de soportes de información; gestión de cambios; mantenimiento de equipos y programas; metodología de análisis y evaluación de riesgos; manual de medidas de seguridad; plan de contingencia; etc. Entre los técnicos: controles de acceso lógico; normas de diseño, desarrollo y, sobre todo, mantenimiento de programas propios; tipo de técnicas criptográficas y casos en que procede su uso; etc. Entre los físicos: controles de acceso físico (personas y objetos); gestión de bienes; protección de fuegos, inundaciones y atentados; etc. Por lo que respecta a los de personal: contratación; plan de concienciación y formación; responsabilidades; infracciones y sanciones; etc.

Por último, el programa de seguridad debe contener las indicaciones oportunas que permitan su implantación y evaluación continuada (entre otros mediante auditorías y cuestionarios periódicos a ser cumplimentados por los responsables de los distintos servicios y secciones), que permitan la actualización del mismo, o incluso de la política de seguridad cuando sea preciso.

Plan de formación

El plan de formación contendrá todas las acciones a desarrollar para la capacitación de todos los trabajadores de la organización en materias de protección y seguridad de la información de forma general y muy especialmente en relación con los puestos de trabajo en concreto. En esta formación se utilizarán diversos métodos como seminarios, cursos, conferencias, demostraciones prácticas y otros. El plan de

formación y su aplicación serán objeto de aprobación y control por parte de las distintas instancias de la propia organización.

Definición y términos de programas destructores

Existen diferentes versiones en cuanto al surgimiento de los programas destructores, sin embargo existen dos hechos que los medios especializados en informática, divulgan como los posibles creadores de estos programas.

El primer hecho es que John Von Neumann, en 1949 en su libro "Theory And Organization of Complicated Automata" describió algunos programas que se reproducían a sí mismos.

El segundo hecho y al parecer el que desencadenó en el mundo de las microcomputadoras a los programas destructores relata que varios científicos de los Laboratorios Bell, inventaron un juego, con el objetivo de entretenerse, inspirado en un programa escrito en Lenguaje Ensamblador, el cual tenía la capacidad de reproducirse cada vez que se ejecutaba.

El juego consistía en invadir la computadora del adversario con un código que contenía una serie de informaciones destinadas a destruir la información de la memoria de su adversario o impedir su correcto funcionamiento. Conscientes de la peligrosidad que el juego representaba, prometieron mantenerlo en secreto.

Sin embargo, en 1983 el Doctor Ken Thompson, en una alocución en la Association For Computing Machinery, da a conocer la existencia de esos programas con detalles de su estructura.

A partir de ese momento, muchos son los casos conocidos de autores de programas destructores, que como recreación o de forma maliciosa han causado el pánico y la histeria en el mundo informático.

Existen varias clasificaciones y definiciones de los mismos según su forma de actuar, nosotros preferimos la siguiente clasificación:

- **Gusanos:**

Los Gusanos son programas que pueden provocar efectos tan dañinos como los causados por los virus, pero se diferencian de éstos en su forma de transmitirse, pues no infectan otros programas con una copia de sí mismos, ni son insertados en otros programas por sus autores. Es decir, no necesitan de otros para propagarse.

Funcionan en grandes sistemas informáticos conectados mediante una red de comunicaciones, difundiéndose rápidamente a través de ésta. Estos programas hacen una gran utilización de los recursos de la red provocando un descenso en la velocidad de funcionamiento de la misma y bloqueos de los sistemas.

- **Caballos de Troya:**

Elementos de Arquitectura y Seguridad Informática

Los Caballos de Troya son conocidos así porque su mecanismo de acción es similar al utilizado por los griegos para entrar en Troya. Sus autores los introducen en programas, generalmente muy utilizados por el dominio público, para que sean propagados a través de copias de los mismos que realicen los usuarios. Es decir, no son capaces de autopropagarse y han sido diseñados generalmente para destruir la información almacenada en los discos.

• **Bombas lógicas y de tiempo:**

Las Bombas Lógicas y Bombas de Tiempo son casos particulares de Caballos de Troya. Bajo ciertas condiciones aparentan mal funcionamiento de la microcomputadora y provocan errores en el funcionamiento de los programas, que van haciéndose cada vez más frecuentes y dañinos hasta causar la destrucción total de la información.

Una Bomba de Tiempo se activa en una fecha u hora determinada, mientras que una Bomba Lógica se activa al darse una condición específica, como puede ser el número de accesos al disco, una determinada combinación de teclas que sea presionada, o cualquier otra condición que se le ocurra a su programador.

• **Joke:**

Los "JOKE" son programas que se han desarrollado con el objetivo de hacer bromas que consisten generalmente en simular efectos propios de los virus, por lo que los usuarios asumen que sus microcomputadoras han sido infectadas. Algunos de estos programas simulan bombas lógicas o de tiempo.

• **Virus:**

Los Virus Informáticos son aquellos programas capaces de reproducirse a sí mismos sin que el usuario esté consciente de ello. Estos se adicionan a programas de aplicación o documentos con macros, así como a componentes ejecutables del Sistema de forma tal que puedan tomar el control de este último durante la ejecución del programa infectado. El código del virus se ejecuta antes que el del programa original y una vez que haya realizado la acción para la que fue diseñado le da el control a este programa, con el objetivo de que el usuario no note su presencia. Un virus al igual que un programa puede realizar tantas cosas como su autor entienda. Por ejemplo:

- 1 Borrar información.
- 2 Formatear un disco.
- 3 Alterar información.
- 4 Hacer más lenta la microcomputadora. etc.

Generalmente los virus poseen dos fases de trabajo:

Fase de Infección: Esta es la más importante y la razón de la existencia del virus. Su objetivo es lograr propagar su código a través de los programas que se encuentran

dentro del Sistema y en los disquetes que sean insertadas en las microcomputadoras. Generalmente los virus colocan en las zonas infectadas unos códigos o marcas de infección con el objetivo de no reinfectarlas. El virus puede propagarse durante semanas o meses sin que el usuario se percate de ello.

Fase de Acción: Esta fase no tiene que estar presente necesariamente en todos los virus. Consiste en toda la acción que no intervenga en el mecanismo de réplica del virus. La activación de la misma es causada por la ocurrencia de alguna o varias condiciones que el código del virus chequea. Estas pueden ser la hora o la fecha actual del Sistema, número de infecciones realizadas, la detección de la ejecución de productos antivirus o de monitoreo a través de "debuggers", etc. Generalmente durante esta fase ocurre la pérdida de la información almacenada en los discos de las microcomputadoras y se ven mensajes o "efectos especiales" en la pantalla.

Un concepto importante es que los virus, como son programas, tienen que cargarse en la memoria de la microcomputadora para poder desarrollar sus fases de trabajo. Atendiendo a este concepto, los virus pueden clasificarse en virus de **Acción Directa** o **Indirecta**.

Los virus de **Acción Directa** son aquellos que se ejecutan sólo cada vez que un programa infectado es ejecutado. Es decir, tanto la fase de infección, que consiste generalmente en la búsqueda de un programa no infectado en el directorio implícito, como la fase de acción del virus, sólo podrán llevarse a cabo en el momento en que el programa infectado es cargado en la memoria y ejecutado. El virus no queda residente en la memoria.

Los virus de **Acción Indirecta** se instalan residentes en la memoria, interceptando una o más interrupciones, una vez que un programa infectado es ejecutado o se inicialice el Sistema desde un disco infectado. A partir de este momento el virus queda residente en memoria y monitorea algunas actividades del Sistema Operativo mientras no se apague la microcomputadora. El virus se propaga mediante la infección de programas (generalmente cuando son ejecutados) o del BOOT Sector de arranque de los disquetes que sean insertados en las torres. Estos virus generalmente antes de intentar quedarse residentes en la memoria RAM averiguan si ya se encontraban instalados en la misma.

Por otra parte, atendiendo a lo que infectan los virus, se clasifican a su vez en tres categorías:

1. Virus Infectores del Sector de Arranque
 2. Virus Infectores de Ficheros Ejecutables
 3. Virus Macro
- **VIRUS QUE INFECTAN SECTORES DE ARRANQUE.**

Estos virus afectan tanto al Sector de Particiones (MASTER BOOT SECTOR), como al Sector de Arranque del S.O. (DOS BOOT SECTOR).

Elementos de Arquitectura y Seguridad Informática

Virus del Sector de Particiones:

El Sector de Particiones se encuentra en el primer sector físico del disco duro. Cuando una microcomputadora es inicializada, lee el Sector de Particiones del disco duro, carga su contenido en la memoria RAM y luego carga el BOOT SECTOR del S.O. que se encuentre en la partición activa ("bootable").

Un virus de este tipo reemplaza el Sector de Particiones por el código del virus y salva el original en otra zona del disco. De esta forma, el virus queda residente en memoria en el momento de la inicialización. La gran mayoría de estos virus son también infectores del Sector de Arranque del S.O. de los disquetes, su tamaño no rebasa los 512 bytes y no necesitan sectores adicionales para guardar el resto de su código. La dirección donde el virus salva en el disco el Sector de Particiones original y el resto de su código se guarda en el Sector de Particiones infectado.

Virus del Sector de Arranque del S.O.:

El Sector de Arranque del S.O. es el primer sector lógico de un disquete y de cada partición en un disco duro. Cuando la microcomputadora es inicializada, lee el sector de arranque de la partición activa del disco duro (después de haber leído la Tabla de particiones) o de un disquete colocado en la torre A.

Estos virus reemplazan el código original del S.O. que hay en esa zona del disco, con su código y trasladan el original a otra zona del disco desde la cual puedan leerlo. Algunos de estos virus necesitan, además del Sector de Arranque, otros sectores para almacenar el resto de su código. Dichos sectores son generalmente marcados como malos en la FAT para que el Sistema Operativo no pueda escribir en ellos. Tanto el sector donde está salvado el Sector de Arranque del S.O. original como aquellos donde está almacenado el resto del código del virus son direccionados por el propio virus en el momento en el que la microcomputadora sea inicializada. Las direcciones de dichos sectores se guardan en el Sector de Arranque del S.O. infectado. De esto se deduce que el virus se carga en la memoria de la microcomputadora en el momento de la inicialización y generalmente permanece en ella hasta que la microcomputadora sea apagada.

- **VIRUS QUE INFECTAN FICHEROS EJECUTABLES.**

Virus del Sistema Operativo:

Estos virus atacan al menos uno de los módulos del Sistema Operativo o de los manipuladores (DEVICE DRIVERS) y pueden infectar intérpretes de comandos (ej: COMMAND.COM), rutinas de Entrada/Salida del Sistema, o manipuladores de propósitos especiales para un Hardware específico. Los virus toman el control durante la inicialización del Sistema Operativo. Esta clase de virus espera por la inserción de disquetes Sistema en una de las torres y en ese caso se replican a sí mismos dentro de los ficheros del S.O.

Virus de Aplicaciones genéricas:

Los virus que infectan aplicaciones genéricas, son capaces de infectar programas de aplicación (generalmente ficheros con extensión .COM, .EXE, Overlay DRV y .DLL). Ellos toman el control cuando un programa infectado es ejecutado. A partir de este momento según haya sido diseñada su fase de infección, infectan a otros programas de aplicación no contaminados que sean ejecutados o accedidos o buscan, en el disco duro instalado o en los disquetes insertados en las torres, aquellos sin infectar para propagarse. Cuando los encuentran se integran al nuevo programa infectándolos y convirtiéndolos en transmisores del virus. Después que el virus explora e infecta, generalmente devuelve el control al código original del programa de aplicación.

Los virus infectan generalmente a los programas adicionando, insertando, o sobrescribiendo su código al del programa. En los dos primeros casos los virus cambian las primeras instrucciones de un programa infectado por otras nuevas, las cuales desvían el control hacia donde reside el resto del código del virus en el momento de la ejecución del programa. Después de la ejecución del virus, las instrucciones originales del programa son restauradas en la memoria y el control es devuelto a éste.

Añadiendo el código:

En la mayoría de los casos los virus sustituyen los primeros bytes del código del programa por una instrucción de salto a la dirección de inicio del código del virus, salvando el contenido original de estos bytes. Normalmente el código del virus se añade al final del programa, aumentando generalmente su tamaño.

De esta forma al ejecutar el programa, se ejecuta primero el código del virus, el cual una vez concluida su acción repone los bytes iniciales del código del programa en memoria y por último le da el control al programa original de forma que éste sea ejecutado normalmente sin provocar sospechas en el usuario.

Insertando su código:

En este caso, el menos común, los virus tienen que localizar programas con espacio libre de forma tal que su código pueda ser totalmente almacenado en éste. El tamaño de los programas infectados no es alterado.

Sobrescribiendo el código:

El virus sobrescribe parcial o totalmente el **código del programa infectado**. De esta forma los programas infectados quedan **dañados irreparablemente** después de la infección y generalmente sus tamaños **no sufren alteración a no ser** que sean menores que el código del virus.

• VIRUS MACRO:

Han transcurrido pocos años desde que fue **reportado por primera vez** en 1995 el virus macro CONCEPT y la cantidad de virus **que utilizan esta técnica** ya sobrepasa los 3000. La organización especializada **National Computer Security Association** informó en Abril de 1997 que según un estudio realizado el **80 %** de las infecciones reportadas eran por causa de estos virus. En los listados de virus más prevalecientes

Elementos de Arquitectura y Seguridad Informática

durante 1997, 1998 y 1999 los virus macro han ocupado los primeros lugares y las estadísticas demuestran que son creados más de 130 virus mensualmente con un índice de crecimiento superior a la de los virus que infectan programas y los infectores de sectores de arranque.

Método de propagación:

Un documento de Word infectado por un virus macro siempre está basado en una plantilla que contiene un conjunto de macros destinadas a realizar la acción de propagación del virus y en ocasiones destruir información. Los creadores de estos virus generalmente aprovechan la existencia de las llamadas "automacros" (AutoExec, AutoOpen, AutoClose, AutoNew y AutoExit) que como su prefijo indica, son ejecutadas de manera automática, por ejemplo cuando un documento es abierto.

En la mayoría de los casos la macro AutoOpen es utilizada para copiar desde el documento infectado hacia la plantilla global, las macros que componen el virus con el fin de que permanezcan "residentes" en la memoria y puedan infectar a otros documentos cuando sean invocadas. Las macros más usadas para este último propósito son las referenciadas como "macros de sistema" que realizan operaciones normalmente ejecutadas al seleccionar opciones en un menú. Entre las más conocidas se encuentran FileClose (Cerrar), FileSave (Guardar) y FileSaveAs (GuardarComo). De esta manera, si un virus inserta una versión propia del FileSave en el NORMAL.DOT, podrá controlar cuando esta opción es pedida por el usuario y en ese momento realizará la infección del documento copiando las macros infectadas desde la plantilla global hacia este último. Como indicamos anteriormente el virus tiene que garantizar que la estructura del documento a infectar sea la correspondiente a una plantilla y por tal motivo hace la conversión de la misma.

¿Como conocer la presencia de virus en nuestro sistema?

Partiendo del hecho real de que cualquier infección de un virus deja una huella, y que algunos virus al activarse manifiestan su presencia, se puede concluir que existen diferentes métodos para detectarlos:

1. A partir de manifestaciones anormales en el funcionamiento del sistema, muchas de las cuales son propias de una contaminación. Por ejemplo:
2. Se observan en la pantalla mensajes ajenos al programa que se está ejecutando, así como de efectos especiales: peloticas saltando, letras cayendo, etc.
3. Mensajes de error en la pantalla relacionados con operaciones de escritura, sobre disquetes protegidos físicamente contra escritura, cuando éstas no debieran ser ejecutadas.
4. Se imprimen caracteres intercambiados en la pantalla o en la impresora.

5. Las luces indicadoras de acceso a las torres de los discos, se encienden cuando no se utilizan.
6. Disminución de la velocidad de operación de la microcomputadora.
7. Los programas funcionan mal o no pueden ser ejecutados.
8. Los programas se demoran más en cargar.
9. Los programas son borrados sin motivo.
10. Alteración en el tamaño de los ficheros, en la hora o la fecha de creación de los mismos, en
11. sus atributos sin que el usuario intervenga.
12. El código de los ficheros es reemplazado por caracteres extraños.
13. Hay una disminución injustificable de la cantidad de memoria disponible para el usuario.
14. Hay una disminución injustificable de la capacidad de almacenamiento de los discos.
15. Pérdida parcial o total de la información almacenada en los discos.
16. Los discos dejan de ser "BOOTABLES".
17. A través de la utilización de productos antivirus identificadores capaces de determinar qué virus ha causado la infección.
18. Con el uso de programas antivirus detectores genéricos, capaces de detectar alteraciones en las zonas sensibles a la contaminación y que son periódicamente controladas por ellos.
19. Mediante los programas que permiten visualizar la estructura de los discos ("Norton Utilities").
20. Analizando los datos brindados por comandos del S.O. que chequean el estado de la estructura del disco, tanto del espacio ocupado como del disponible.
21. Con las comparaciones byte a byte entre dos ficheros supuestamente iguales. Este proceso se puede realizar utilizando los comandos del S.O. El fichero obtenido de la fuente más confiable debe ser tomado como patrón en dicha comparación.
22. Por medio de programas que analicen la utilización de la memoria de la microcomputadora como el SYSINFO de Norton.
23. A través del uso del comando DIR del DOS con el fin de comprobar alteraciones en el tamaño de los programas.

Daños más comunes ocasionados por los virus

Los daños ocasionados por un virus son evaluados a través de las implicaciones

Elementos de Arquitectura y Seguridad Informática

económicas que representan la pérdida parcial o total de los recursos y horas hombre-máquina invertidos tanto durante el proceso de diseño, puesta a punto e implantación de las aplicaciones y sus datos, como las que se derivan de los gastos en que se incurran durante el proceso de recuperación de un sistema infectado.

Los gastos en el proceso de recuperación dependen de los daños ocasionados por el virus tanto en su fase de infección como en la de activación, así como del nivel de organización en la salva de la información que tenga el usuario. Además, existen virus que son difíciles de detectar y que de una forma muy solapada alteran la información almacenada en los discos.

Nota: En Junio de 1998 se detectó el virus CIH, el primero virus desarrollado para dañar el Hardware de la microcomputadora. Esto lo logra mediante la modificación por sobre escritura del programa (BIOS), contenido en la pastilla de memoria 'FLASH BIOS', cuya función es controlar todo el trabajo de la computadora. Esta acción dañina pudiera requerir en algunos casos que la tarjeta madre 'motherboard' tenga que ser reemplazada, siendo un efecto similar al que ocasionaría un daño físico en un dispositivo electrónico. El creador del virus se basó en el hecho de que a través de los años se ha visto una tendencia a facilitar la escritura en la BIOS. La tecnología de la 'FLASH ROM' permite que el contenido de la BIOS pueda ser modificado por el usuario final de la computadora, ya sea con el fin realizar nuevas actualizaciones o de corregir errores. Este proceso se realiza con la ayuda de un programa distribuido por los fabricantes de 'Hardware' y existen sitios en INTERNET destinados a tal efecto. Desde el punto de vista electrónico, el voltaje de habilitación de escritura de este tipo de memoria ya se ha estandarizado a 5V, que es el mismo que utiliza la mayoría de los circuitos integrados conectados en la 'motherboard', por lo que muchos fabricantes conectan directamente este voltaje a la terminal de habilitación de escritura de la memoria y ésta queda habilitada físicamente para la escritura.

Otros creadores de virus han comenzado a incorporar este mecanismo de destrucción a sus virus, ejemplo de ellos son los virus Emperor y W97/II-S. Se espera que en un futuro aparezcan más virus con estas característica.

Software antivirus. Clasificación.

Preventores

Los programas que previenen la infección quedan residentes en la memoria de la computadora todo el tiempo, y monitorean algunas de las funciones del sistema. Todos estos programas antivirus esperan por la indicación de que un virus está intentando infiltrarse en el sistema, lo cual casi siempre es indicado por un intento de acceso a uno de los programas ejecutables de la microcomputadora, al Sector de Arranque del S.O., al Sector de Particiones o al Sistema Operativo. Además monitorean los programas que se cargan en la memoria y los documentos Word que se abren, chequean llamadas a funciones del sistema, y mantienen el control sobre

la tabla de vectores de interrupción, entre otras cuestiones. Cuando ocurre una de estas acciones, el programa bloquea el sistema y muestra un mensaje de advertencia al usuario.

Estos productos presentan la dificultad de provocar cierta molestia en el trabajo de los usuarios debido a que existen programas que necesitan realizar algunas de estas acciones para poder trabajar, por lo que pueden ocurrir repetidamente falsas alarmas. Además son incapaces de prevenir inicialmente la infección del sistema por los virus infectores del Sector de Arranque ya que ésta se produce en el proceso de inicialización del Sistema, cuando todavía el programa preventivo no puede estar residente en memoria.

Actualmente existen virus que utilizan técnicas capaces de burlar a muchos de estos programas ya que realizan la infección a través de accesos no convencionales a los servicios del BIOS y del S.O.

Estos programas deben quedar residentes en la memoria tan pronto haya concluido el proceso de inicialización del Sistema.

Conclusiones:

- Se instalan residentes en la memoria con el fin de controlar el estado del sistema y detectar acciones sospechosas.
- Ocupan memoria.
- Pueden provocar falsas alarmas ocasionando molestias a los usuarios.
- Pueden interferir en el funcionamiento del sistema u otros programas.

Identificadores

Estos productos Antivirus identifican virus específicos que infectan al sistema. Los mismos trabajan con las características de un virus o variantes de un determinado virus, y exploran el sistema buscando cadenas (secuencias de bytes) de código particulares, o patrones característicos de los mismos para identificarlos. Estas cadenas o patrones de búsqueda son almacenados en bases de datos que pueden encontrarse dentro del propio programa .identificador o en ficheros de datos externos. El hecho de que estos programas sólo identifiquen los virus conocidos por sus creadores provoca que sean inefectivos contra el resto de los virus, de ahí que requieran una constante actualización. La mayoría de estos productos revisan el Sector de Particiones (discos duros), el Sector de Arranque del S.O. y los ficheros ejecutables y overlays del disco seleccionado, cuando son ejecutados y los ficheros documentos de Word cuando son abiertos. Además, generalmente chequean la memoria para buscar y desactivar a los virus que identifican, antes de revisar el disco. Esto es debido a que existen virus que infectan a los programas una vez que los mismos son abiertos, por lo que un producto antivirus de este tipo, que no chequee la memoria, se convierte en una herramienta de propagación de dichos virus ya que en la medida en que los ficheros son "abiertos", son infectados.

Elementos de Arquitectura y Seguridad Informática

Además los virus que utilizan la técnica STEALTH son capaces de desinfectar a los ficheros contaminados en la medida en que sean "abiertos", por lo que los mismos no son detectados como infectados.

El método más seguro para utilizar estos productos es el de ejecutarlos una vez que la microcomputadora haya sido encendida teniendo colocado un disquete Sistema original con protección física de escritura en la torre A. De esta forma se garantiza que no exista algún virus residente en la memoria en el momento en que el identificador es ejecutado.

Algunos identificadores revisan los programas en el momento en que son ejecutados y los ficheros documentos Word cuando son abiertos, o cuando son copiados hacia el disco duro, con el objetivo de evitar la propagación de los virus que identifican. Además pueden revisar el BOOT SECTOR de los disquetes en el momento en se realice un acceso a ellos.

Conclusiones :

- Identifican virus conocidos en las áreas del sistema sensibles a las infecciones de los virus.
- Requieren de constante actualización.
- Son inefectivos contra virus desconocidos.
- Utilizados correctamente pueden prevenir infecciones y/o reinfecciones por virus conocidos.

Descontaminadores

Sus características son similares a los productos identificadores con la diferencia de que su principal función es descontaminar a un sistema, que ha sido infectado, eliminando el virus y retornando el sistema a su estado original por lo que tienen que ser muy precisos en la identificación de los virus contra los que descontaminan. Generalmente estos programas le brindan al usuario la posibilidad de ejecutarlos solamente como identificadores, o sea sin realizar la descontaminación. Estos productos presentan las mismas desventajas que los identificadores y sus reglas de utilización son similares a los mismos.

La descontaminación utilizando estos productos sólo es recomendable cuando no existe otra forma de recuperarse de la infección como puede ser el caso de la inexistencia de copias de programas de aplicación confiables desde donde se puedan restaurar los programas infectados o cuando el proceso de restauración desde copias originales resulta muy trabajoso y costoso debido a la gran propagación de la infección. No siempre se garantiza una total restauración de las condiciones originales del Sistema.

Conclusiones:

- Sus características son similares a las de los identificadores. Su función principal es la descontaminación.
- Tienen que ser precisos en la identificación de los virus y sus variantes.
- No garantizan un 100 % la recuperación del estado inicial del sistema.

Detectores genéricos

Los productos detectores genéricos detectan alteraciones en las zonas más vulnerables del sistema: los ficheros de inicialización del Sistema Operativo, los programas de aplicación, los ficheros documentos Word, el Sector de Particiones y el Sector de Arranque del S.O. de los discos. La infección de un virus puede ser comprobada, detectando las modificaciones o alteraciones provocadas por éste durante el proceso de infección. Por tal motivo los programas detectores toman como patrón, en el momento de su instalación, toda la información del sistema que los virus pueden afectar y mediante la ejecución de forma periódica de una rutina de chequeo comparan el estado actual del sistema, con el estado "patrón".

La mayoría de estos programas realizan el chequeo sólo cuando son ejecutados. Otros permanecen residentes en la memoria chequeando constantemente las zonas "vulnerables" a los virus y no permiten que sean ejecutados programas diferentes a los controlados o que hayan sido alterados.

Aunque los detectores genéricos son productos antivirus muy efectivos en la lucha contra los virus informáticos, ya que en ocasiones, dada la información que almacenan pueden restaurar los daños ocasionados por los virus, presentan la dificultad de que para realizar su proceso de chequeo tienen que partir de patrones, los cuales pueden resultar falsos patrones. Esto provoca que siempre se debe partir de programas originales y microcomputadoras cuyos discos duros hayan sido recientemente revisados contra virus.

Otra dificultad es que al chequear alteraciones en los ficheros dejan al usuario la decisión de considerar el fichero alterado como sospechoso.

Estos programas deben tener implementadas técnicas capaces de luchar contra los virus que una vez instalados en la memoria, al detectar que un fichero es abierto, lo desinfecten, por lo que puede provocar que el programa detector no encuentra ninguna alteración en los parámetros del fichero a revisar y no sea capaz de detectar la infección.

Conclusiones:

- Detectan alteraciones en las zonas del sistema sensibles a las infecciones de los virus.
- Toman como patrón un sistema limpio y realizan comparaciones contra dicho patrón.

Elementos de Arquitectura y Seguridad Informática

- No identifican a los virus que realizan la infección.
- No requieren de constantes actualizaciones.
- Algunos por la información que guardan pueden descontaminar genéricamente un sistema.

Recuperadores

Estos programas constituyen un caso particular de productos Antivirus. Sus características se basan en la posibilidad de restaurar las condiciones iniciales del sistema una vez que éste ha sufrido alteraciones debido a la acción de un virus. Esta posibilidad viene dada por el hecho de que:

- Algunos virus guardan información de los ficheros de datos que alteran, con el objetivo de restaurarlos cuando el usuario intente verificarlos y de esta forma tratar de ocultar la infección.
- Existen otros cuyos autores se han propuesto vender los productos que recuperen la información destruida por el virus durante su fase de activación o infección.

En ocasiones estos programas una vez que hayan realizado su labor de restauración tienen que ejecutar un proceso de descontaminación.

En la actualidad se han desarrollado programas recuperadores que guardan en bases de datos, creadas al efecto, la información referente al nombre de los ficheros que se encuentran contenidos en el disco, sus tamaños, sus bytes iniciales y el valor correspondiente a la suma de chequeo calculada basándose en el código del fichero. Con esta información se pueden restaurar la mayoría de los ficheros infectados por los virus actualmente detectados. Estos programas además pueden guardar una copia original del Sector de Particiones de los discos duros y del Sector de Arranque del S.O. de los discos. El proceso de recuperación en este caso consiste en sobrescribir el Sector de Arranque infectado, con las copias originales.

Los programas recuperadores, a diferencia de los descontaminadores no son capaces de eliminar todos los efectos provocados por una infección en particular, ya que no identifican qué virus fue el que realizó la infección.

Conclusiones:

- Su función es recuperar la información dañada por la acción de un virus.
- Una recuperación de este tipo sólo es posible cuando el creador del virus concibe la destrucción de la información de forma tal que pueda ser recuperada. Ejemplo: virus DBASE.

- Una vez concluido el proceso de recuperación de la información se debe proceder a su chequeo para evitar reinfecciones o nuevos daños. Ejemplo: virus DISK KILLER.

Vacunas

Muchos de los virus informáticos al infectar a un programa dejan una "marca" para identificar que éste ha sido contaminado por él y no reinfectarlo. Este hecho ha sido utilizado por los programadores para crear las llamadas "vacunas" antivirus, las cuales en la mayoría de los casos consisten en un código "parásito" (generalmente pocos bytes) que se incorpora a los programas para protegerlos de la contaminación de un determinado virus.

Otro tipo de marca muy utilizado por los virus es el cambio de los valores correspondientes a la hora o la fecha de creación del programa que ha sido infectado, por un valor fijo y en este caso la vacuna consiste en hacer lo mismo a los ficheros que se desean proteger de esos virus. Esta característica que presentan los virus de utilizar marcas que identifican la infección, es inherente a todas las clasificaciones de virus.

Este método de protección en sus inicios fue muy utilizado pero con la aparición de nuevos virus se demostró que era poco práctico y tenía muchas inconveniencias:

Por lo general cada virus utiliza su propia marca de infección, es decir, generalmente la utilizada por él para identificar la infección no es utilizada por ningún otro virus. Esto provoca que existan gran cantidad de marcas de infección, lo que trae aparejado la existencia de sus correspondientes vacunas.

Sector de Arranque del S.O., el Sector de Particiones, los ficheros del Sistema y los programas de aplicaciones dejan de ser originales (patrones) ya que sufren alguna alteración con respecto a su estado inicial de acuerdo a las vacunas que le sean aplicadas. (Por ejemplo un programa "vacunado" contra el virus JERUSALEM es aumentado en 5 bytes).

En ocasiones unas vacunas desactivan a otras, por ejemplo si las alteraciones realizadas por nuevas vacunas ocurren en las mismas posiciones en que fueron realizadas las anteriores solamente tendría efecto la última de estas vacunas. Por ejemplo un programa .COM vacunado contra el virus JERUSALEM, que sea nuevamente vacunado contra otro virus, de forma tal que la marca sea colocada a continuación de la vacuna contra el JERUSALEM, (al final del fichero) podrá ser infectado por dicho virus, ya que éste busca su marca de infección al final del fichero y en esta posición se encuentra la marca de la nueva vacuna.

Un programa infectado por un determinado virus puede ser nuevamente contaminado por éste si el programa es vacunado contra otro virus.

La utilización de vacunas en el Sector de Arranque y en el Sector de Particiones puede provocar que los discos o disquetes vacunados dejen de ser "BOOTABLES".

Elementos de Arquitectura y Seguridad Informática

En ocasiones el uso de vacunas puede provocar dificultades para la descontaminación de los programas infectados (cuando se utilizan programas descontaminadores).

En la actualidad existe un nuevo tipo de vacuna que consiste en la inserción de una rutina de integridad y un código de chequeo en los programas. Esta rutina revisa si han ocurrido alteraciones en el programa cuando el mismo es ejecutado. El chequeo es realizado contra el código insertado. Esta nueva técnica no evita la contaminación de los ficheros, sino que detecta cualquier alteración en los mismos.

Conclusiones:

- Consisten en un código parásito (generalmente de pocos bytes) que se incorpora a los programas para protegerlos de la infección de un virus específico, ya conocido
- Aunque inicialmente constituyeron un método efectivo para evitar infecciones de virus conocidos, en la actualidad son consideradas totalmente obsoletas.
- Entre otros inconvenientes presentan los siguientes:
- Las zonas vacunadas dejan de ser originales:
- Ocasionalmente unas vacunas desactivan a otras.
- Ocasionalmente permiten reinfecciones.

¿Cómo actuar ante una infección?

Cuando es detectada la infección en una microcomputadora, pueden ocurrir tres casos generales:

El virus que realizó la infección es reconocido por un programa descontaminador, que posee el usuario, capaz de restaurar las condiciones del sistema antes de la infección. Esto ocurre cuando el virus no destruye información durante sus fases de infección o activación.

El virus que realizó la infección es o no reconocido por un programa identificador/descontaminador, que posee el usuario, incapaz de restaurar las condiciones del sistema antes de la infección, pero es posible realizar la recuperación del sistema a través de copias de seguridad o patrones salvados.

El virus que realizó la infección es reconocido o no por un programa identificador/descontaminador, que posee el usuario, incapaz de restaurar las condiciones del sistema antes de la infección, pero no es posible realizar la recuperación del sistema a través de copias de seguridad o patrones salvados.

Anexos

Anexo 1: Diccionario del Hardware

Éste es un diccionario muy particular; como su nombre indica, no encontrará todos los términos propios de la informática, sino "sólo" aquellos que conciernen al hardware, especialmente las **siglas**, de oscuro significado, especialmente si se desconoce el idioma inglés.

Aparecen no sólo aparatos y dispositivos, sino también palabras que hacen alusión a protocolos, normas, o bien términos del software muy básicos o cuya relación con el hardware hace imprescindible conocer su significado.

286: microprocesador (CPU) de 16 bits tanto interna como externamente; sin caché ni coprocesador matemático integrados. Inventado por Intel, existe de otras muchas marcas.

386: microprocesador (CPU) de 32 bits tanto interna como externamente; sin caché ni coprocesador matemático integrados. Inventado por Intel, existe de otras marcas como AMD.

386SX: microprocesador (CPU) de 32 bits internamente y 16 externamente; sin caché ni coprocesador matemático integrados. Inventado por Intel.

486: microprocesador (CPU) de 32 bits tanto interna como externamente; con caché y coprocesador matemático integrados según modelo (DX o SX). Inventado por Intel, existe de otras marcas como AMD, Cyrix o Texas Instruments.

486DX: microprocesador (CPU) de 32 bits tanto interna como externamente; versión con caché y coprocesador matemático integrados. Inventado por Intel, existe de otras marcas como AMD, Cyrix o Texas Instruments.

486DX2: microprocesador (CPU) de 32 bits tanto interna como externamente; con caché y coprocesador matemático integrados y el doble de velocidad internamente (DX2) que a nivel placa. Inventado por Intel, existe de otras marcas como AMD, Cyrix, Texas Instruments.

486DX4: microprocesador (CPU) de 32 bits tanto interna como externamente; con caché y coprocesador matemático integrados y el triple de velocidad internamente que a nivel placa. Inventado por Intel, existe de otras marcas como AMD, Cyrix, Texas Instruments.

486SX: microprocesador (CPU) de 32 bits tanto interna como externamente; con caché interna pero sin coprocesador matemático integrado. Inventado por Intel, existe de otras marcas como Cyrix.

8086: microprocesador (CPU) de 16 bits internamente y 8 externamente; sin caché ni coprocesador matemático integrados. Inventado por Intel.

Elementos de Arquitectura y Seguridad Informática

8088: microprocesador (CPU) de 8 bits tanto interna como externamente; sin caché ni coprocesador matemático integrados. Inventado por Intel.

80286: denominación oficial completa del 286.

80386: denominación oficial completa del 386.

80486: denominación oficial completa del 486.

A: la letra que designa a la primera disquetera en el sistema operativo DOS.

ACPI: Advanced Configuration and Power Interface, un sistema por el cual en los ordenadores más modernos se puede controlar el consumo eléctrico del ordenador por software.

AGP: Advanced Graphics Port, o Puerto Avanzado para Gráficos. Tipo de slot dedicado en exclusiva a tarjetas gráficas, de prestaciones iguales o superiores al PCI dependiendo de la versión de AGP que se trate (1x o 2x).

ASCII: uno de los primeros y más usados códigos de caracteres. Existe en versiones de 7 u 8 bits.

AT: Advanced Technology, tipo de ordenador compatible con el AT original de IBM; en general, cualquier ordenador compatible con un micro 286.

ATA: Advanced Technology Attachment, dispositivo conector de tecnología avanzada. El estándar en que se basa la tecnología IDE.

ATA-2: extensión del estándar ATA para diseño de dispositivos IDE que añade modos PIO hasta el PIO-4 y la definición del modo de acceso LBA.

ATA-3: última revisión del estándar ATA para diseño de dispositivos IDE que añade mayor fiabilidad en los modos PIO y DMA avanzados, así como SMART para el análisis de fallos.

ATAPI: Advanced Technology Attachment Packet Interface, paquete interfaz del dispositivo conector de tecnología avanzada. El estándar que designa los dispositivos que pueden conectarse a controladoras ATA (IDE), como por ejemplo lectores de CD-ROM.

ATX: formato de placa base bastante moderno cuyas principales características son una mejor ventilación y accesibilidad, además del uso de clavijas mini-DIN y una gran integración de componentes.

B: la letra que designa a la segunda disquetera en el sistema operativo DOS.

Baby-AT: el formato de placa base más extendido en el mundo PC, en progresiva sustitución por el ATX, del que se diferencia entre otras cosas por usar clavija DIN ancha para el teclado y tener una peor disposición de los componentes.

baudio: el equivalente a un bit en comunicaciones.

BASIC: uno de los primeros lenguajes de programación, de uso muy sencillo.

BEDO: Burst-EDO, tipo de memoria RAM, de mejores características que la DRAM, FPM y EDO y similares o mejores que la SDRAM.

BIOS: Basic Input-Output System, sistema básico de entrada-salida. Programa incorporado en un chip de la placa base que se encarga de realizar las funciones básicas de manejo y configuración del ordenador.

bit: unidad mínima de información de la memoria, equivalente a un "sí" (0) o un "no" (1) binarios. La unión de 8 bits da lugar a un byte.

bps: bits por segundo, unidad de transmisión de datos, empleada principalmente en referencia a módems o comunicaciones de red.

buffer: memoria dedicada a almacenar temporalmente la información que debe procesar un dispositivo hardware para que éste pueda hacerlo sin bajar el rendimiento de la transferencia. Aparece típicamente en discos duros y CD-ROMs.

burst: palabra inglesa que significa a ráfagas.

bus: canal por el que circula información electrónica en forma de bits. El ancho de bus es el número de bits transmitidos simultáneamente por el bus.

byte: unidad de información, compuesta de 8 bits consecutivos. Cada byte puede representar, por ejemplo, una letra.

C: (1) la letra que designa a la primera unidad de disco duro o a la primera partición activa de éste en el sistema operativo DOS.

C: (2) uno de los lenguajes de programación más utilizados en la actualidad.

caché: cualquier tipo de memoria "intermedia" entre dos aparatos, que acelera las comunicaciones y transmisiones de datos entre ellos. Por extensión, se aplica a la "caché de nivel 2", es decir, la que está en la placa base, entre el microprocesador y la memoria.

CAD: Computer Assisted Draw, dibujo asistido por ordenador; generalmente se refiere al específicamente arquitectónico o ingenieril.

CELP: tipo de zócalo para memoria caché en módulos.

CGA: Computer Graphics Array, o dispositivo gráfico para computadoras. Un tipo de tarjeta gráfica capaz de obtener 320x200 puntos con 4 colores o 640x200 con 2 colores.

CISC: Complex Instruction Set Chip, un tipo de microprocesador que entiende instrucciones muy largas y complejas, aunque no es capaz de ejecutarlas a tanta velocidad como un CISC.

clónico: ordenador montado a partir de piezas de terceros fabricantes, en el cual no existe tecnología aportada por el ensamblador; también denominado ordenador

Elementos de Arquitectura y Seguridad Informática

ensamblado. También, componente mimetizado por un fabricante a partir del modelo original de otro con el que es compatible.

CMOS: Complementary Metal Oxide Semiconductor, un tipo de memoria que se caracteriza por consumir muy poca energía eléctrica, lo que la hace idónea para almacenar datos de la BIOS.

COAST: tipo de zócalo para memoria caché en módulos.

COM: acrónimo con el que se designa a cada uno de los puertos series o de COMunicaciones.

CON: nombre con el que el DOS se refiere a la pantalla o al teclado, según se trate de un dispositivo de destino o fuente de los datos.

controlador: forma española de denominar los drivers.

coprocesador: cualquier microchip que realice una operación especializada, ayudando o liberando al microprocesador principal de realizarla. Generalmente, se entiende por tal al específicamente "matemático", aunque en la actualidad éste suele venir integrado en el micro principal.

cps: caracteres por segundo que puede escribir una impresora.

CPU: Central Processing Unit o Unidad Central de Proceso. El "cerebro" de un ordenador; en general, sinónimo de microprocesador. En ocasiones se usa para referirse al toda la caja que contiene la placa base, el micro y las tarjetas de expansión.

cracker: un hacker con intenciones destructivas o delictivas.

CRT: Cathodic Ray Tube, tubo de rayos catódicos. La tecnología empleada en los televisores y en los monitores clásicos.

DIMM: tipo de conector para memoria RAM; los módulos a conectar tienen 168 contactos.

disipador: aparato que ayuda a eliminar el calor generado por un cuerpo, en general el microprocesador del equipo, en ocasiones con la colaboración de un ventilador. Para ello, busca tener buena conducción del calor (suelen ser de cobre) y gran superficie.

DMA: Direct Memory Access, acceso directo a memoria. Método de gestionar los dispositivos hardware por el cual pueden acceder directamente a la memoria sin precisar que el microprocesador gestione el proceso.

docking station: denominación habitual de un dispositivo para ordenadores portátiles que les dota de diversos conectores (teclado, ratón, monitor, ranuras PCI...) permitiendo utilizar el portátil como si fuera un ordenador de sobremesa.

DOS: un sistema operativo para PC, monousuario y monotarea, del que deriva el Windows 95. Existen versiones del DOS de Microsoft, IBM y Digital Research, entre otros.

dot pitch: o ancho de punto. La distancia entre dos fósforos del mismo color en una pantalla; cuanto menor sea, mayor nitidez.

dpi: dots per inch, puntos por pulgada (en español, ppp). Número de puntos que imprime una impresora en cada pulgada; 300 dpi significa 300x300 puntos en cada pulgada cuadrada.

DRAM: el tipo de memoria RAM original, de peores características que FPM, EDO o SDRAM. A veces se usa este término incorrectamente para referirse a la FPM.

driver: pequeño programa cuya función es controlar el funcionamiento de un dispositivo del ordenador bajo un determinado sistema operativo.

DSTN: ver "Dual Scan".

Dual-Scan: tipo de pantalla para portátil; hoy en día es el estándar. La calidad de imagen depende bastante de la iluminación exterior.

DVD: Digital Video Device, dispositivo digital de vídeo. Dispositivo óptico de almacenamiento masivo capaz de albergar entre 4,7 y 17 GB en cada disco de 12 cm (de apariencia similar a los CDs).

DX: siglas con las que se conoce a los procesadores 386 ó 486 "completos" de Intel, aquellos que no son versiones de capacidades reducidas (falta de coprocesador en los 486 o bus externo de 16 bits en los 386).

ECP: Extended Capability Port, puerto de capacidad extendida. Tipo de puerto paralelo compatible con el original pero que ofrece mayores prestaciones de velocidad, así como bidireccionalidad.

EDO: tipo de memoria RAM, de mejores características que la DRAM y FPM pero inferior a la SDRAM.

EGA: Extended Graphics Array, o dispositivo gráfico extendido. Un tipo de tarjeta gráfica capaz de obtener hasta 640x350 puntos con 16 colores.

EIDE: Enhanced IDE, o IDE mejorado. Actualmente el estándar para manejo de discos duros; también llamado Atapi o Ata-4. Permite manejar hasta 4 dispositivos (discos duros, CD-ROMs...) en dos canales IDE separados, cada uno con su interrupción IRQ correspondiente. En la actualidad, casi todos los PCs llevan una controladora EIDE integrada en la placa base.

EISA: Extended-ISA, tipo de slot para tarjetas de ampliación basado en el estándar ISA pero de 32 bits y capaz de 32 MB/s de transferencia; actualmente en desuso debido a la implantación del PCI.

EMS: memoria expandida, un tipo de memoria superior (por encima de los primeros 640 Kb), bien mediante hardware o imitada por software como el EMM386.EXE.

Elementos de Arquitectura y Seguridad Informática

entrelazado: sistema en desuso consistente en dibujar en el monitor primero todas las líneas horizontales pares y después las impares, consiguiendo altas resoluciones a bajo precio pero con gran cansancio visual.

EPP: Enhanced Paralel Port, puerto paralelo mejorado. Tipo de puerto paralelo compatible con el original pero que ofrece mayores prestaciones de velocidad, así como bidireccionalidad.

escaner: aparato capaz de introducir información óptica (documentos, fotos...) en el ordenador.

ESDI: Enhanced Small Device Interface, interface mejorada para pequeños dispositivos. Antigua tecnología para el diseño y manejo de dispositivos, generalmente discos duros, hoy totalmente en desuso.

Ethernet: un estándar para redes de ordenadores muy utilizado por su aceptable velocidad y bajo coste. Admite distintas velocidades según el tipo de hardware utilizado, siendo las más comunes 10 Mbits/s y 100 Mbits/s (comúnmente denominadas Ethernet y Fast Ethernet respectivamente).

FAST-ATA II: ATA rápido Véase Enhanced IDE.

FAT: tabla de asignación de archivos Tabla oculta de cada unidad de asignación en un disco flexible o duro. La FAT registra la forma en que los archivos están almacenados en diferentes y no necesariamente necesariamente contiguas unidades de asignación. Los virus también suelen ocultarse en la FAT; asegúrese de que el software de verificación de virus revise la tabla en busca de programas malignos.

Una tabla de asignación de archivos se vale de un método sencillo para mantener el registro de los datos. La dirección de la primera unidad de asignación del archivo se guarda en el archivo de directorios. En la entrada de la FAT para la primera unidad de asignación está la dirección de la segunda unidad de asignación utilizada para almacenar el archivo. En la entrada de la segunda unidad de asignación está la dirección de la tercera, y así sucesivamente hasta la última entrada de unidad de asignación, la que contiene un código de fin de archivo. Puesto que esta tabla es la única manera de saber la forma en que se localizan los datos dentro del disco, el DOS crea y mantiene dos copias de la FAT por si alguna de ellas se daña.

FDD: Floppy Disk Device, forma inglesa de denominar la disquetera.

FireWire: "cable de fuego" o "IEEE 1394", un estándar para la conexión de dispositivos al ordenador, tanto interna como externamente. De muy reciente aparición, está muy poco extendido pero se prevee que sustituya a EIDE y SCSI, con velocidades teóricas empezando en 25 MB/s y quizá llegando hasta 1 GB/s.

flash-BIOS: una BIOS implementada en flash-ROM.

flash-ROM: un tipo de memoria que no se borra al apagar el ordenador, pero que puede modificarse mediante el software adecuado.

FLOP: Floating-Point Operation, operación de coma flotante; cada una de las operaciones matemáticas de dicha clase que es capaz de realizar un microprocesador. Se usa para medir el rendimiento del mismo, generalmente en millones de FLOPs (MFLOPs).

floppy: forma inglesa de denominar al disquete.

FM: tipo de tecnología utilizado en tarjetas de sonido de gama media, consistente en reproducir el sonido mediante un sintetizador musical FM, obteniendo un resultado menos real que el ofrecido por las tarjetas wave table.

FPM: Fast Page Mode, tipo de memoria RAM, de mejores características que la DRAM pero inferior a la EDO o SDRAM. A veces se denomina (incorrectamente) DRAM.

FX: siglas que designan un tipo de chipset de Intel para Pentium, conocido comercialmente como "Tritón" y hoy en día en desuso.

GB: gigabyte, Unidad de medición. Se usa al establecer una cantidad de memoria o la capacidad de un disco múltiplo del byte equivalente a 1024 megabytes. Más correcta, aunque menos utilizada, es la forma Gb. Coloquialmente, giga.

GUI: Graphical User Interface, interfaz gráfica de usuario. Programa software que gestiona la interacción con el usuario de manera gráfica mediante el uso de iconos, menús, ratón...

GAME PORT PUERTO DE JUEGOS: Un receptáculo que permite utilizar una palanca, un yugo de control, o algún otro dispositivo para juegos de computadora.

hacker: experto informático especialista en entrar en sistemas ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos o simplemente para demostrar que es capaz de hacerlo.

hardware: la parte física del ordenador (placa, micro, tarjetas, monitor...).

HDD: Hard Disk Device, forma inglesa de denominar al disco duro.

Hércules: tipo de tarjeta gráfica capaz de obtener 720x350 puntos con 2 colores.

HSP: tipo de módem que utiliza parte de las capacidades del microprocesador y del sistema operativo (generalmente Windows 95) para realizar tareas que en otros módems realizarían chips especiales, reduciendo su precio a costa de perder versatilidad y precisar micros potentes.

HX: siglas que designan un tipo de chipset de Intel para Pentium, conocido comercialmente como "Tritón II"; de mayor rendimiento que los FX y VX, hoy en día está en desuso.

Hz: hertzio, unidad de medida de la frecuencia equivalente a 1/segundo. Utilizado principalmente para los refrescos de pantalla de los monitores, en los que se considera 60 Hz (redibujar 60 veces la pantalla cada segundo) como el mínimo aconsejable.

Elementos de Arquitectura y Seguridad Informática

I/O: Input/Output, entrada/salida. Generalmente hace referencia a dispositivos o puertos de comunicación (serie, paralelo, joystick...) o a la tarjeta que los controla (si no están integrados en la placa base).

IA32: Intel Architecture 32, el conjunto de instrucciones de 32 bits que entienden los microprocesadores compatibles Intel.

IA64: Intel Architecture 64, el conjunto de instrucciones de 64 bits que se diseña para los futuros microprocesadores compatibles Intel de 64 bits, como el Merced.

IDE: Integrated Drive Electronics, disco con la electrónica integrada. Una tecnología para el diseño y manejo de dispositivos, generalmente discos duros; hoy en día el estándar entre los ordenadores PCs de prestaciones "normales". El número máximo de dispositivos que pueden ser manejados por una controladora IDE es de 2, mientras que si es EIDE pueden ser hasta 4.

IPW: Incremental Packet Writer, grabador incremental de paquetes. Un método utilizado en grabadoras de CD-ROM modernas para gestionar más eficazmente la escritura de los datos.

IRQ: Interrupt ReQuest, solicitud de interrupción. Cada uno de los canales usados para gestionar muchos dispositivos hardware, como tarjetas de expansión o controladoras. En los antiguos XT eran 8, en ordenadores ATs y superiores 16 (de la 0 a la 15).

ISA: Industry Standard Architecture, un tipo de slot o ranura de expansión de 16 bits capaz de ofrecer hasta 16 MB/s a 8 MHz.

ISDN: la palabra inglesa para "RDSI".

Jaz: dispositivo de almacenamiento de datos, consistente en una unidad lectora-grabadora y un soporte de datos en forma de cartucho de unas 3.5 pulgadas y capacidad 1 ó 2 GB. Ideado por la empresa Iomega.

Jumper: caballete de conexión Conector eléctrico que permite a un usuario seleccionar una configuración particular en una tarjeta de circuitos. El caballete de conexión es un pequeño rectángulo de plástico con dos o tres receptáculos. Para instalarlo, basta con que lo empuje hacia abajo contra dos o tres pins de varios que salen hacia arriba desde la superficie de la tarjeta de circuitos. La colocación del caballete completa el circuito electrónico para la configuración deseada.

jumper settings: parámetros del caballete de conexión La configuración de los conductores móviles en un adaptador. Estos parámetros dictan la forma en que un adaptador interactúa con el resto de un sistema, determinando, por ejemplo, el canal de solicitud de interrupciones (IRQ).

Joint Photographic Experts Group (JPEG) graphic gráfico JPEG: Un formato gráfico ideal para imágenes complejas de las escenas naturales del mundo real, como fotografías, arte realista y pinturas. (El formato no es muy adecuado para los trazos con rectas, el texto, o caricaturas sencillas.) Desarrollado por el Grupo de Expertos en Fotografía Unidos (JPEG), comité creado por dos cuerpos de estándares internacionales, el formato gráfico JPEG utiliza la compresión libre. Utiliza una propiedad conocida de la visión humana, el hecho de que los pequeños cambios de color son menos observables que los cambios de brillo; la compresión JPEG no es observable a menos que se utilicen razones altas de compresión. Por lo general, JPEG puede lograr razones de compresión de 10:1 o 20:1 sin una degradación notable en la calidad de la imagen; ésta es una mejor razón de compresión que la del Formato de Intercambio de Gráficos (GIF).

Joint Photographic Experts Group (JPEG) Grupo de Expertos en Fotografía Unidos
Un comité de expertos en gráficos por computadora, patrocinado en forma conjunta por la Organización Internacional de Estándares (ISO) y el Comité Consultivo Internacional sobre Telefonía y Telegrafía (CCITT), que ha desarrollado el estándar para gráficos JPEG.

K, Kb Abreviatura de kilobyte, múltiplo del byte equivalente a 1024 bytes. Más correcta, aunque menos utilizada, es la forma "kb"; también se emplea "Kb".

kilobyte (K): Unidad básica de medida para la memoria de las computadoras y la capacidad de los discos; equivale a 1,024 bytes. El prefijo kilo- indica 1,000, pero el mundo de las computadoras trabaja con doses, no con dieces: 210 = 1,024. Ya que un byte es lo mismo que un carácter en computación personal, 1 K de datos puede contener 1,024 caracteres (letras, números o signos de puntuación).

keyboard teclado: El dispositivo de entrada más empleado de cualquier computadora. El teclado proporciona un conjunto de teclas alfabéticas, numéricas, de puntuación, de símbolos y de control. Cuando se presiona una tecla de carácter, se envía una señal de código de entrada a la computadora, la que repite la señal mostrando un carácter en la pantalla. Véase autorepeat key, keyboard layout y toggle key.

keystroke tecleo: Acción física de presionar una tecla para introducir un carácter o iniciar un comando.

keystroke buffer búfer de tecleo: Área de almacenamiento en memoria empleada para guardar los tecleos cuando el usuario escribe algo mientras el microprocesador está ocupado. Por ejemplo, si comienza a escribir mientras se guarda un archivo, los caracteres escritos se colocan en este búfer. Una vez que se llena (por lo general el búfer puede contener 20 caracteres), se escucha un sonido cada vez que se oprime otra tecla, lo que indica que ya no se acepta dicha entrada. Cuando el microprocesador termina su tarea, los caracteres del búfer son enviados a la pantalla.

K5: microprocesador de AMD similar al Pentium clásico.

Elementos de Arquitectura y Seguridad Informática

K6: microprocesador de AMD que incluye MMX, de rendimiento superior al Pentium MMX aunque inferior al Pentium II.

K6-2: también llamado "K6-3D"; microprocesador de AMD que incluye MMX y la tecnología "3DNow!" para el manejo de aplicaciones 3D, de rendimiento igual o superior al Pentium II.

local area network (LAN) red de área local: Una red de ordenadores de tamaño medio, dispersa por un edificio o incluso por toda una ciudad. Computadoras personales y de otros tipos enlazadas, dentro de un área limitada, mediante cables de alto desempeño para que los usuarios puedan intercambiar información, compartir periféricos y extraer programas y datos almacenados en una computadora dedicada, llamada servidor de archivos.

Con una enorme gama de tamaños y complejidades, las LANs pueden vincular desde unas cuantas computadoras personales hasta un costoso periférico compartido, como una impresora láser. Los sistemas más complejos usan computadoras centrales (servidores de archivos) y permiten que los usuarios se comuniquen unos con otros a través de correo electrónico para compartir programas multiusuario y acceder bases de datos compartidas. Véase AppleTalk, baseband, broadband, bus network, EtherNet, multiuser system, NetWare, network operating system (NOS), peer-to-peer network, ring network y star network.

laptop computer computadora laptop: Pequeña computadora portátil cuya ligereza le permite al usuario colocarla en las rodillas. A las computadoras laptop pequeñas, que pesan menos de 3 kg y caben en un portafolios, se les conoce como computadoras notebook, mientras que a las más pequeñas, que pesan alrededor de 2.5 kg, se les denomina computadoras subnotebook.

laser printer (impresora láser): Impresora de alta resolución que usa una versión de la tecnología de reproducción electrostática de las máquinas copiadoras para grabar texto e imágenes gráficas en una página.

Para imprimir una página, los circuitos del controlador de la impresora reciben las instrucciones de impresión desde la computadora y construyen un mapa de bits de cada punto en una página. El controlador asegura que el mecanismo de impresión láser transfiera una réplica precisa de este mapa de bits a un tambor o cinturón sensibilizado fotostáticamente. Activado y desactivado con rapidez, el haz cruza el tambor, y a medida que aquél se mueve, el tambor carga las áreas que quedan expuestas al haz. Las áreas cargadas atraen el tóner (tinta cargada eléctricamente) mientras el tambor gira y pasa por el cartucho de tóner. Un alambre cargado eléctricamente atrae el tóner desde el tambor hacia el papel, y unos rodillos calientes funden el tóner en el papel. Un segundo alambre cargado eléctricamente neutraliza la carga eléctrica del tambor.

landing zone (zona de aterrizaje): En forma ideal, la única área de la superficie de un disco duro que toca en realidad la cabeza de lectura/escritura. A través del proceso de estacionamiento de la cabeza, la cabeza de lectura/escritura se mueve sobre la zona de aterrizaje antes de apagar la computadora, y se desplaza para reposar ahí. La zona de aterrizaje, que no tiene datos codificados, está diseñada de modo que evite que la cabeza de lectura/escritura dañe las porciones del disco utilizadas para guardar datos una colisión de la cabeza.

LBA: Logical Block Address, direcciones de bloques lógicas. Tecnología usada en los discos duros de más de 528 MB para superar la limitación a este tamaño que la BIOS y el DOS les impondrían.

LCD: Liquid Crystal Display, pantalla de cristal líquido. Tecnología electrónica que permite crear pantallas planas.

LED: Light Emitting Diode, diodo emisor de luz. Un dispositivo luminoso de pequeño tamaño utilizado en electrónica.

LINUX: un sistema operativo multiusuario y multitarea basado en UNIX.

LPT: una forma de denominar a los puertos paralelo (LPT1, LPT2...).

LPX: un formato de placas base.

master: el nombre asignado al primero de los dos dispositivos de un canal IDE, en contraste al "slave", que es el segundo.

MB: megabyte, múltiplo del byte equivalente a 1024 kilobytes. Más correcta, aunque menos utilizada, es la forma "Mb". Coloquialmente, "mega".

MFLOP: un millón de FLOPs; ver FLOP.

MFM: un tipo muy antiguo de controladora para disco duro, previo al IDE.

MGA: Monochrome Graphics Adapter, adaptador de pantalla monocromo. La primera tarjeta gráfica usada en los PC, capaz de funcionar sólo en modo de texto monocromo.

MHz: megahertzio, múltiplo del hertzio igual a 1 millón de hertzios. Utilizado para medir la "velocidad bruta" de los microprocesadores.

Micro Channell: un tipo de slot o ranura de expansión de 32 bits capaz de ofrecer hasta 40 MB/s a 10 MHz. En desuso, tuvo poco éxito debido a ser un diseño propiedad exclusiva de IBM.

MIDI: Interface Digital para Instrumentos de Música, utilizado para manejar audio digitalmente con la ayuda de ordenadores u otros instrumentos electrónicos (teclados, samplers...).

MIPS: Millones de Instrucciones Por Segundo que puede realizar un microprocesador, una medida del rendimiento del mismo.

Elementos de Arquitectura y Seguridad Informática

MMX: MultiMedia eXtensions, grupo de instrucciones para microprocesador desarrolladas por Intel que incrementan el rendimiento multimedia de los microprocesadores que las soportan.

módem: MODulador-DEModulador, dispositivo hardware que transforma las señales digitales del ordenador en señal telefónica analógica y viceversa.

MPEG:

multimedia: el conjunto de imagen, sonido y vídeo aplicado al PC.

NE-2000:

Net PC:

ns: nanosegundo, submúltiplo del segundo igual a 10^{-9} elevado a menos 9 segundos.

NTSC: sistema de codificación de la señal televisiva utilizado mayoritariamente en EEUU.

OCR: Optic Character Recognition, reconocimiento óptico de caracteres, asociado usualmente a la digitalización de textos mediante escáner; convierte la "foto" digital del texto en texto editable con un procesador de texto.

OEM: aquellos componentes provenientes de la venta al por mayor, por lo que carecen de ciertos extras que puedan tener las versiones en caja individual.

OSD: "On Screen Display", o "presentación (de datos) en pantalla". Método con el que algunos monitores (y televisores) presentan los datos de ajuste de los mismos en la propia pantalla, generalmente superpuestos a la imagen.

overclocking: técnica por la cual se fuerza un microprocesador a trabajar por encima de su velocidad nominal.

OverDrive: familia de microprocesadores de Intel dedicada a la actualización de equipos. Existen con núcleos de 486 y de Pentium con o sin MMX.

P&P: ver "Plug and (&) Play".

PAL: sistema de codificación de la señal televisiva utilizado mayoritariamente en Europa.

PC: Personal Computer, ordenador personal; nombre (registrado) con que bautizó IBM en 1.981 al que se convertiría en estándar de la informática de usuario; por extensión, cualquier ordenador compatible de otra marca basado en principios similares.

PCI: un tipo de slot o ranura de expansión de 32 bits capaz de ofrecer hasta 132 MB/s a 33 MHz.

PCMCIA: Personal Computer Memory Card International Association, el estándar para conectar y dispositivos de tamaño tarjeta de crédito utilizados en ordenadores portátiles.

PDA: Personal Digital Assistant, un tipo de micro ordenador portátil de tamaño muy reducido que generalmente se controla mediante una pantalla táctil.

Pentium: microprocesador de Intel de 32 bits con arquitectura superescalar, capaz de hacer el procesamiento paralelo de dos instrucciones por ciclo de reloj y con una unidad matemática muy mejorada respecto de la del 486.

pin: cada uno de los conectores eléctricos de muchos elementos hardware, como las "patitas" de muchos microprocesadores.

PIO: tecnología utilizada en los discos duros IDE modernos para elevar la tasa de transferencia teórica máxima hasta 16,6 MB/s en los modelos que cumplen con el modo más avanzado, el "PIO-4".

pipeline: entubamiento En un diseño de computadora, línea de ensamble en el microprocesador que reduce en forma drástica la velocidad de procesamiento de las instrucciones mediante la recuperación, ejecución y reescritura. Utilizado durante mucho tiempo en UNIX, el entubamiento que se incluye con el Intel 80486 permite procesar una instrucción en cada ciclo del reloj. El microprocesador Intel Pentium tiene dos entubamientos, uno para datos y otro para instrucciones, por lo que puede procesar dos instrucciones (una por entubamiento) en cada ciclo de reloj. Se dice que un microprocesador con dos o más entubamientos emplea arquitectura superescalar.

pipeline stall : entubamiento atascado Un error en un microprocesador equipado con arquitectura superescalar que retrasa el procesamiento de una instrucción. En un microprocesador con un diseño de ejecución en orden, como Pentium, las instrucciones deben procesarse en un orden preciso, y un atascamiento en un entubamiento también retrasaría el proceso en el otro entubamiento. En un esquema de ejecución sin orden, un atascamiento en un entubamiento no detiene al otro.

pipelining entubamiento Un método de diseño de un microprocesador que permite a éste controlar más de una instrucción a la vez. Existen por lo general cinco pasos secuenciales del control de una instrucción por parte de un microprocesador, y un esquema de entubamiento permite que una de cada cinco instrucciones pase por uno de los pasos durante un ciclo de reloj. Los microprocesadores con arquitectura superescalar tienen dos o más entubamientos, lo que incrementa aún más la eficiencia.

pitch: o "dot-pitch", la distancia entre dos puntos ("dots") del mismo color. También denominado ancho de punto.

pixel: cada uno de los puntos individuales representados en una pantalla de ordenador.

Plug and Play: tecnología que permite la autodetección de dispositivos tales como tarjetas de expansión por parte del ordenador, con objeto de facilitar su instalación.

Elementos de Arquitectura y Seguridad Informática

PnP: ver "Plug and (N) Play".

POST: Power On Self Test, el test que realiza la BIOS del ordenador a los dispositivos al arrancar.

PPP: Point to Point Protocol, protocolo de comunicaciones en el que se basan muchas redes.

ppp: "puntos por pulgada" (en inglés, "dpi"). Número de puntos que imprime una impresora en cada pulgada; "300 dpi" significa 300x300 puntos en cada pulgada cuadrada.

PRN: nombre con el que el DOS se refiere al puerto de impresora en uso (LPT1 u otro).

protocolo: protocolo Conjunto de estándares para el intercambio de información entre dos sistemas de computación o dos dispositivos de computadora. Véase communications protocol, file transfer protocol (FTP) e Internet.

propietario: dicese del diseño o elemento cuya licencia de utilización y desarrollo no es pública, sino que es explotado por una empresa en exclusiva.

PS/2: una gama de ordenadores de IBM. Debido a la utilización generalizada en ellos de ratones con clavija mini-DIN, por extensión se utiliza para referirse a este tipo de conector.

RAM: Random Access Memory, o Memoria de Acceso aleatorio. La memoria principal en la que se almacenan los datos durante el funcionamiento de un ordenador, la cual se borra al apagarlo. De diversos tipos (Fast Page, EDO, SRAM...) y conectores (SIMM; DIMM...).

RAMDAC: conversor analógico-digital (DAC) de la memoria RAM, empleado en las tarjetas gráficas para transformar la señal digital con que trabaja el ordenador en una salida analógica que pueda entender el monitor.

RDSI: Red Digital de Servicios Integrados, las líneas digitales de teléfono, con caudales típicos de 64 ó 128 Kbps (kilobaudios por segundo).

refresh rate: tasa de refresco de pantalla; el número de veces por segundo que se dibuja en el monitor una pantalla. Cuanto mayor sea, mejor; se mide en hertzios (Hz).

RISC: Reduced Instruction Set Chip, un tipo de microprocesador que entiende sólo unas pocas instrucciones pero que es capaz de ejecutarlas a gran velocidad.

RLL: Véase Run-Length Limited (RLL).

ROM: Read Only Memory, o Memoria de sólo lectura. Un tipo de memoria "estática", es decir, que no se borra al apagar el ordenador y en principio en la que no puede escribirse, salvo que se empleen métodos especiales. Usada sobre todo para guardar la BIOS del ordenador.

RS232: el tipo estándar de puerto serie.

SAI: Sistema de Alimentación Ininterrumpida. Aparato que protege al ordenador de cambios bruscos del flujo eléctrico, a la vez que previene cualquier carencia del mismo.

SB 16: SoundBlaster 16, una tarjeta de sonido de 16 bits de Creative Labs en la que se basa el actual estándar para tarjetas de sonido del que toma el nombre.

scanner: aparato capaz de digitalizar información; usualmente se refiere al que es capaz de digitalizar imágenes, textos o fotos.

SCSI: Small Computer Systems Interface, tecnología para el manejo de dispositivos, tanto interna como externamente. Permite manejar hasta 7 discos duros, CD-ROMs, escáners... Más rápida y versátil que IDE, es el estándar para ordenadores de alta gama, tanto PCs como Apple Machintosh, servidores UNIX, etc.

SDRAM: DRAM Síncrona, tipo de memoria RAM de mejores características que la DRAM, FPM y EDO.

SGRAM: tipo de memoria usada para labores de vídeo, basada en la SDRAM. De mejores características que la FPM, EDO, VRAM, WRAM y SDRAM.

shareware: una forma de distribución de software, basada en poder probarlo un tiempo antes de decidirnos a comprarlo. No confundir con freeware (software gratuito).

SÍMM: tipo de conector para memoria RAM. Existe en versiones para módulos de 30 y 72 contactos.

SL: siglas que hacen referencia a microprocesadores con características de ahorro energético, capaces de utilizar el Suspend Mode para reducir su actividad hasta prácticamente detenerse.

slave: el nombre asignado al segundo de los dos dispositivos de un canal IDE, en contraste al "master", que es el primero.

slot: o ranura de expansión; cada uno de los conectores donde se enchufan ("pinchan") las tarjetas de expansión. De forma alargada y longitud variable, según la tecnología a la que pertenezcan: ISA, EISA, VESA, PCI, AGP...

socket: palabra inglesa que significa zócalo (generalmente el del microprocesador).

software: los programas de ordenador, la lógica que le permite realizar tareas al hardware (la parte física).

speaker: palabra inglesa que significa altavoz. En general designa al pequeño altavoz interno del ordenador o PC-speaker.

SPP: Standard Parallel Port, la forma actual de denominar al tipo estándar de puerto paralelo para distinguirlo de otras versiones más avanzadas como ECP o EPP.

Elementos de Arquitectura y Seguridad Informática

SRAM: Static-RAM, RAM estática. Un tipo de memoria de gran velocidad usada generalmente para memoria caché.

super-Disk: dispositivo de almacenamiento de datos, consistente en una unidad lectora-grabadora y un soporte de datos de forma y tamaño similares a un disquete de 3.5 pulgadas y capacidad 120 MB. Ideado por la empresa Imation, mantiene la compatibilidad con los disquetes clásicos de 3,5 pulgadas.

SVGA: tipo de tarjeta gráfica capaz de obtener hasta 800x600 puntos en 16 colores.

SX: siglas con las que se conoce a los procesadores 386 ó 486 "económicos" de Intel, aquellos que son versiones de capacidades reducidas (falta de coprocesador en los 486 o bus externo de 16 bits en los 386).

terminador: pequeño aparato electrónico basado en resistencias eléctricas, usado en redes de cable coaxial para terminar la cadena de ordenadores conectados de forma abierta (sin hacer un anillo).

TFT: o matriz activa. Tipo de pantalla para portátil; de mayor precio que las Dual Scan, la calidad de imagen no depende de la iluminación exterior como en éstas.

trackball: aparato apuntador similar al ratón en el que se desplaza con la mano, el pulgar o el índice una bola acoplada a una base que permanece fija.

Tritón: forma comercial de designar a una serie de chipsets de Intel, los FX, VX y HX.

TWAIN: Technology Without An Interesting Name, "tecnología sin un nombre interesante". Peculiar denominación para el estándar de drivers para escáners.

TX: siglas que designan el último de los chipsets para Pentium fabricado por Intel, caracterizado por soportar memorias SDRAM y optimizado para micros MMX, pero con un bus máximo de 66 MHz.

UART: el chip que controla los puertos serie.

UDF: Universal Disk Format, un método derivado del IPW que se utiliza en grabadoras de CD-ROM modernas para gestionar más eficazmente la escritura de los datos. Ideal para realizar grabaciones en múltiples sesiones.

Ultra-DMA: tecnología utilizada en los discos duros IDE más modernos para elevar la tasa de transferencia teórica máxima hasta 33 MB/s.

UNIX: un sistema operativo multiusuario y multitarea.

USB: Universal Serial Bus, bus serie universal. Tipo de conector que puede soportar hasta 126 periféricos externos, con un ancho de banda a compartir de 1,5 MB/s, lo que lo hace especialmente indicado para ratones, impresoras, joysticks o módems.

V.32bis: una norma internacional para comunicaciones vía módem que permite alcanzar una velocidad de 14.400 baudios.

V.34: una norma internacional para comunicaciones vía módem que permite alcanzar una velocidad de 28.800 baudios.

V.34+: una norma internacional para comunicaciones vía módem que permite alcanzar una velocidad de 33.600 baudios.

V.90: una norma internacional para comunicaciones vía módem que permite alcanzar una velocidad máxima de 55.600 baudios, dependiendo de ciertas condiciones, sobre todo tipo y calidad de la línea.

VESA: (1) un estándar de modos de vídeo para tarjetas VGA y superiores, que permite programar drivers compatibles con todas las tarjetas gráficas que cumplan estas normas, independientemente del chip que incorporen.

VESA: (2) ver VLB, Vesa Local Bus.

V.Fast Class (V.FC) Protocolo de modulación patentado utilizado por varios fabricantes de módems antes de que se publicara el estándar V.34. La mayor parte de los módems V.FC se pueden actualizar para ajustarse por completo a V.34.

VGA: Video Graphics Array, o dispositivo Gráfico de Vídeo. Un tipo de tarjeta gráfica capaz de obtener hasta 640x480 puntos en 16 colores (en el modelo estándar original).

virtual (dispositivo): el que se imita mediante software y las capacidades de los otros dispositivos sí existentes, como por ejemplo un coprocesador matemático imitado por Linux mediante el microprocesador.

virtual (memoria): la que se imita por software a partir del disco duro.

VLB: o Vesa Local Bus, un tipo de slot o ranura de expansión de 32 bits capaz de ofrecer hasta 132 MB/s a 33 MHz o 160 MB/s a 40 MHz.

VRAM: tipo de memoria usada para labores de vídeo. De mejores características que la FPM y EDO.

VRM: módulo de voltajes de micro.

VX: siglas que designan un tipo de chipset de Intel para Pentium, conocido comercialmente como "Tritón III"; de mayor rendimiento que el FX, hoy en día en desuso.

WAN: Wide Area Net, red de área ancha. Una red de ordenadores de muy gran tamaño, dispersa por un país o incluso por todo el planeta.

WAV: el tipo de archivo de sonido más común, caracterizado por ofrecer una gran calidad pero sin compresión de los datos.

wave table: tabla de ondas. Tipo de tecnología utilizado en tarjetas de sonido, consistente en utilizar para la reproducción del sonido muestras reales de instrumentos grabados en la memoria de la tarjeta, obteniendo una calidad mucho mayor que con un sintetizador FM.

Elementos de Arquitectura y Seguridad Informática

WRAM: tipo de memoria usada para labores de vídeo. De mejores características que la FPM y EDO, y algo superior a la VRAM.

WWW: World Wide Web, o "gran telaraña mundial".

WYSIWYG: What You See Is What You Get, es decir, "lo que ve es lo que obtiene". La metodología de los programas de Windows (y Mac y otros, en realidad), consistente en que el resultado final una vez impreso se vea desde el comienzo en la pantalla del ordenador, en contraposición a lo que sucede con los programas para DOS, por ejemplo.

XENIX: un sistema operativo multiusuario y multitarea basado en UNIX.

XGA: eXtended Graphics Array, o dispositivo gráfico extendido. Un tipo de tarjeta gráfica capaz de obtener hasta 1024x768 puntos en 16 colores.

XMS: memoria extendida, una forma de acceder a la memoria superior (por encima de los primeros 640 Kb), mediante software como el HIMEM.SYS.

XT: tipo de ordenador compatible con el modelo denominado de esa forma por IBM. En general, cualquier PC compatible con disco duro y un procesador 8086 o superior.

ZIF: Zero Insertion Force (socket), o zócalo de fuerza de inserción nula. Conector de forma cuadrada en el que se instalan algunos tipos de microprocesador, caracterizado por emplear una palanquita que ayuda a instalarlo sin ejercer presión ("Force") sobre las patillas del chip, muy delicadas.

ZIP: (1) tipo de archivo comprimido. Muy utilizado, especialmente en InterNet, fue ideado por la empresa PKWARE.

Zip: (2) dispositivo de almacenamiento de datos, consistente en una unidad lectora-grabadora y un soporte de datos de forma y tamaño similares a un disquete de 3.5 pulgadas y capacidad 100 MB. Ideado por la empresa Iomega.

Anexo 2: SETUP

Bajo el nombre de **Standard CMOS Setup** o similar, se suele englobar la puesta al día de la fecha y hora del sistema, así como la configuración de discos duros y disqueteras.

A continuación se brinda un resumen de cada una de las posibilidades que brinda este Menú:

Standard CMOS	Opciones de configuración estándar, similares a las de un BIOS PC AT-compatible.
BIOS Features	Opciones ampliadas del BIOS AWARD.
Chipset Features	Opciones específicas al Chipset del sistema.
Power Management	Opciones de administración de la potencia, Advanced Power Management (APM) .
PnP/PCI Configuration	Opciones de configuración del sistema Plug and Play y del Bus Local PCI.
Integrated Peripherals	Configuración del subsistema de E/S, depende de los controladores de periféricos que tenga integrado la tarjeta madre de su sistema. Es posible que esta opción no aparezca en el menú principal, en ese caso la configuración de este subsistema se realiza en el Chipset Features SETUP .
Supervisor/ User Password Setting	Cambia, fija o desactiva la contraseña. En las versiones de BIOS que permiten contraseñas separadas de User y Supervisor , la contraseña del Supervisor permite el acceso al SETUP. La contraseña del User permite generalmente acceso al sistema cuando este se enciende.
IDE HDD Auto Detection	Automáticamente detecta y configura los parámetros del disco duro IDE.
HDD Low Level Format	Esta opción puede no aparecer en algunas versiones de BIOS. La mayoría de los fabricantes de discos IDE recomiendan que no se formateen estos discos a bajo nivel. AWARD suministra este utilitario solamente para personal de servicio.

Elementos de Arquitectura y Seguridad Informática

Load Defaults	BIOS	Carga los valores implícitos del BIOS, los cuales garantizan una operación más estable y un rendimiento mínimo para el sistema.
Load Defaults	Setup	Carga los valores implícitos del SETUP, los cuales garantizan un rendimiento óptimo de las operaciones del sistema.
Save & Setup	Exit	Salva los cambios en la CMOS RAM y sale del SETUP.
Exit Save	Without	Abandona todos los cambios y sale del SETUP.

La pantalla de manejo suele ser similar a ésta:

ROM PCI/ISA BIOS (2A4IBS29)
STANDARD CMOS SETUP
AWARD SOFTWARE, INC.

Date (mm:dd:yy) : Sat, May 2 1998								
Time (hh:mm:ss) : 19 : 54 : 53								
HARD DISKS	TYPE	SIZE	CYLS	HEAD	PRECOMP	LANDZ	SECTOR	MODE
Primary Master	: User	420	986	16	65535	985	52	NORMAL
Primary Slave	: None	0	0	0	0	0	0	-----
Secondary Master	: None	0	0	0	0	0	0	-----
Secondary Slave	: None	0	0	0	0	0	0	-----
Drive A : 1.44M, 3.5 in.								
Drive B : None								
Video : EGA/VGA								
Halt On : All Errors								
				Basic Memory: 640K				
				Extended Memory: 23552K				
				Other Memory: 384K				
				Total Memory: 24576K				
ESC : Quit		↑ ↓ → : Select Item		PU/PD/+/- : Modify				
F1 : Help		(Shift)F2 : Change Color						

Date.

Permite fijar en su computadora la fecha actualizada con la que trabajará su ordenador, la misma se introduce con el siguiente formato: <day>, <date> <month> <year>.

day	El día de la semana, desde Sun (domingo) hasta Sat (Sábado), es determinado por el BIOS y no se puede modificar.
date	La fecha del mes, desde 1 hasta 31 (o el máximo permitido por el mes).
month	El mes, desde Enero hasta Diciembre.
year	El año, desde 1900 hasta 2099.

Time.

Introduce en su computadora la hora actualizada, con el siguiente formato **Hour** (00 a 23), **Minute** (00 a 59), **Second** (00 hasta 59). Note que el tiempo está calculado basándose en la hora militar de 24H. Por ejemplo, la 1P.M son las 13:00:00.

Hard Disk Drivers.

Este campo contiene las especificaciones de los discos que Ud. puede instalar en su sistema. Sobre la Tarjeta Madre existen dos canales IDE PCI, lo cual se refleja físicamente en la existencia de dos conectores, uno para el canal Primario y otro para el canal Secundario. En cada uno de estos canales es posible instalar hasta dos discos duros o lectores de Disco-Compacto, para un total de cuatro dispositivos IDE. Para una correcta instalación de estos dispositivos, en cada canal uno de ellos deben seleccionarse como Amo (Master) y el segundo como Esclavo (Slave).

Para el caso específico de un dispositivo SCSI se pondrá en este campo no instalado (NONE) ya que estos operan usando su propio BIOS. También se debe poner no instalado si no hay disco duro conectado en el sistema.

Existen, por lo general, 46 tipos predefinidos de tipos de disco duros y una entrada (el tipo USER) para ser definida por el usuario. Además en los BIOS actuales existe una opción AUTO, que automáticamente detecta las características del disco duro durante el proceso de carga. Por otra parte en el Menú principal existe la opción **IDE HDD AUTO DETECTION**, que automáticamente fija los valores de la entrada USER.

Presione PgUp o PgDn para seleccionar un tipo de disco duro. Tenga en cuenta que las especificaciones de su disco deben coincidir con los del tipo de disco seleccionado de la tabla. Si las características de su disco no coinciden con ninguno de los de la lista, Ud. puede usar la entrada USER para definir las manualmente o el modo AUTO para hacerlo automáticamente durante el proceso de carga.

Si seleccionó la entrada USER, será necesario introducir manualmente parte de los datos que conforman los parámetros de la geometría del disco (CYLS, HEADS, PRECOMP, LANDZONE, SECTORS). Suministre estos datos directamente desde el teclado y presione <ENTER>. Esta información puede obtenerse en la documentación del disco duro. Para los discos duros actuales los valores de PRECOMP y LANDZONE son irrelevantes, fíjelos a 0, a 65536 o al valor que se corresponde con el último cilindro del disco duro.

Elementos de Arquitectura y Seguridad Informática

A continuación se brinda una breve explicación del significado de cada uno de los parámetros del disco duro.

TYPE	EL BIOS contiene una tabla de tipos de disco predefinidos. Cada uno de los cuales tiene un número específico de cilindros, cabezas, precomp, landzone y sectores. Los discos que no se acomodan a un tipo de esta lista predefinida se conocen como tipo USER (Usuario) y su geometría debe ser introducida manualmente.
CYLS.	Número de Cilindros
HEADS	Número de Cabezas
PRECOMP	Cilindro donde comienza la precompensación de escritura. Esta es una técnica empleada en los antiguos discos duros, para garantizar que existieran la misma cantidad de sectores por pistas, aún en aquellas pistas que tenían menor tamaño (las más cercanas al centro del disco). En sentido general consistía en variar la corriente de escritura para estas pistas, obteniendo un menor campo magnético sobre la superficie. En los discos duros IDE más modernos esta técnica no se emplea porque físicamente no tienen la misma cantidad de sectores por pistas.
LANDZONE	Zona de parqueo de las cabezas (landing zone)
SECTORS	Número de sectores.
SIZE	Es la capacidad del disco duro (aproximadamente). Note que este tamaño es ligeramente mayor que el tamaño de un disco formateado.
MODE	Modo de trabajo del disco: Normal, Large, LBA o Auto.

Los modos de trabajo del disco son:

Auto	El BIOS realiza la autodetección del modo óptimo de trabajo de su disco.
Normal	Para discos cuya capacidad sea menor de 528 MB. Los valores máximos de Cilindros, Cabezas y sectores son 1024, 16 y 63.
LBA	(Logical Block Addressing): Para discos con más de 1024 cilindros, durante los accesos al disco duro, el controlador IDE transforma la dirección descrita por los cilindros, cabezas y sectores en una dirección de bloque físico. Esto aumenta significativamente los rangos de transferencia de datos.
Large	Para discos que no soportan LBA y tienen más de 1024 cilindros.

Nota: El disco no funcionará correctamente si Ud. entra un valor incorrecto para esta categoría, por esta razón es muy recomendable usar cualquiera de los modos automáticos para seleccionar el disco duro.

Driver A/B.

Este campo recoge los tipos de torres de floppy que pueden ser instalados en su computadora, los mismos pueden ser:

None	No hay torre de floppy instalada.
360K, 5.25 in	Torre standard de 5 ¼", 360 KB.
1.2M, 5.25 in	Torre AT de alta densidad 5 ¼", 1.2 MB.
720K, 3.5 in	Torre de baja densidad 3 ½", 720 KB.
1.44M, 3.5 in	Torre de alta densidad 3 ½", 1.44 MB.
2.88M, 3.5 in	Torre de alta densidad 3 ½", 2.88 MB.

Por ejemplo, en la imagen aparece un disco de 420 MB, con 986 cilindros, 16 cabezas... y trabajando en modo Normal, puesto que no supera los 528 MB. Todos estos valores suelen venir en una pegatina adherida al disco duro, o bien se pueden hallar mediante la utilidad de autodetección de discos duros, que se ilustra más adelante.

En cualquier caso, generalmente existe más de una combinación de valores posible. Por cierto, los lectores de CD-ROM de tipo IDE no se suelen configurar en la BIOS; así, aunque realmente ocupan uno de los lugares (usualmente el maestro del segundo canal o el esclavo del primero) se debe dejar dichas casillas en blanco, eligiendo None o Auto como tipo.

Video.

Esta opción selecciona el tipo de monitor primario que ha sido instalado en su computadora, deben coincidir el tipo de monitor instalado con el tipo de adaptador de video. Aunque el BIOS soporta un monitor secundario no es necesario seleccionar su tipo en el SETUP. Normalmente el BIOS es capaz de determinar el tipo del monitor primario, aunque este valor se puede cambiar de forma manual. Los tipos soportados son:

EGA/VGA	Enhanced Graphics Adapter/Video Graphics Array. Para adaptadores EGA, VGA, SVGA o PGA
CGA 40	Para adaptadores Color Graphics Adapter, en el modo de 40 columnas.
CGA 80	Para adaptadores Color Graphics Adapter, en el modo de 80 columnas.
MONO	Para adaptadores Monocromáticos, incluyendo adaptadores Hercules de alta resolución.

Elementos de Arquitectura y Seguridad Informática

Nota: En algunas tarjetas madres antiguas existe un Jumper, normalmente cerca del controlador de teclado, que permite seleccionar también el tipo de monitor instalado. Este selecciona entre un display monocromático (**Mono**) y uno en colores (**Color**). Si este Jumper está mal seleccionado y no se corresponde con la identificación automática que realiza el BIOS durante el POST, este reporta el siguiente error: **"Display Swicht no Proper"**.

Memory.

Esta categoría tiene carácter solamente informativo, ya que la cantidad de memoria instalada es determinada durante el POST que realiza el BIOS cuando se enciende la máquina.

Base Memory: El POST del BIOS determina la cantidad de memoria base (o convencional) instalada en el sistema. El valor típico de esta memoria es 640K.

Extended Memory: El BIOS determina cuanta memoria extendida existe durante el POST. Esta es la cantidad de memoria localizada por arriba del primer megabyte de memoria en el mapa de direcciones del CPU.

Other Memory: Esto se refiere al espacio de memoria localizado en el espacio de direcciones entre los 640 K y los 1024 K. Esta memoria puede ser utilizada por diferentes aplicaciones. El DOS utiliza esta área para cargar los programas residentes y controladores de dispositivos con el objetivo de liberar memoria convencional. El mayor uso de esta área es como Shadow RAM, en el Capítulo siguiente se explicará la forma en que se activa esta Zona como Shadow RAM y las posibilidades que ofrece.

Opciones del Menú BIOS FEATURES SETUP.

ROM PCI/ISA BIOS (2A4IBS29)
 BIOS FEATURES SETUP
 AWARD SOFTWARE, INC.

CPU Internal Cache	: Enabled	Video BIOS Shadow	: Enabled
External Cache	: Enabled	C8000-CFFFF Shadow	: Disabled
Quick Power On Self Test	: Enabled	D0000-D7FFF Shadow	: Disabled
Boot Sequence	: A,C	D8000-DFFFF Shadow	: Disabled
Swap Floppy Drive	: Disabled		
Boot Up NumLock Status	: On		
IDE HDD Block Mode	: Enabled		
Gate A20 Option	: Normal		
Memory Parity Check	: Disabled		
Typeomatic Rate Setting	: Disabled		
Typeomatic Rate (Chars/Sec)	: 6		
Typeomatic Delay (Msec)	: 250		
Security Option	: Setup		
IDE Second Channel Control	: Enabled		
PCI/VGA Palette Snoop	: Disabled		
		ESC : Quit	↑↓ : Select Item
		F1 : Help	PU/PD/!/- : Modify
		F5 : Old Values (Shift)	F2 : Color
		F7 : Load Setup Defaults	

Estas opciones permiten un mayor rendimiento, así como la personalización del trabajo de la computadora según sus necesidades. Algunas de estas Opciones o sus Valores pudieran no estar presente en todas las versiones del SETUP del BIOS AWARD, en ocasiones el nombre de la opción cambia ligeramente, en ese caso hemos puesto los dos nombres y hemos analizado todos sus posibles valores. En todo caso Ud. debe referirse a las opciones que le brinda su SETUP y buscar aquí la información de la opción que le interesa, puesto que hemos hecho una recopilación de varias versiones de SETUP soportadas sobre diferentes tarjetas madres con procesadores diferentes (i486, Pentium, Pentium II).

Virus Warning.

Esta opción protege el Sector de Arranque (Boot Sector) y la Tabla de Particiones del disco, protegiendo a los mismos de modificaciones accidentales o provocadas por virus. Si se detecta un intento de escritura en alguno de ellos, aparece un mensaje como el siguiente, que pide confirmar ("Y") o denegar ("N") la escritura en estas localizaciones. Si Ud. recibe este mensaje, en un momento en el que no está escribiendo en estos sectores, corra alguna aplicación antivirus para localizar el problema

Elementos de Arquitectura y Seguridad Informática

! WARNING!

Disk boot sector is to be modified

Type "Y" to accept write or "N" to abort write

Award Software, Inc.

Los valores permitidos para esta categoría son:

Enabled	Se activa automáticamente cuando el sistema despierta, causando la aparición del mensaje cuando se trata de acceder al Sector de Arranque o la Tabla de Particiones.
Disabled (Implícito)	No aparece el mensaje cuando se trata de acceder al Sector de Arranque o la Tabla de Particiones.

Nota: Esta opción se recomienda inhabilitarla si Ud. va a instalar un nuevo S.O o va a formatear su disco. Es especialmente incompatible con Windows 95, ya que este mensaje se pone en pantalla en modo texto, lo cual entra en conflicto con el modo gráfico del Windows provocando un bloqueo de la máquina, que incluso no se puede relacionar con este mensaje.

CPU Internal Cache/ External Cache.

Estas opciones permiten habilitar (enable) o desactivar (disable) la memoria Cache Interna del CPU (L1) o la memoria Cache Externa (en la actualidad del tipo PDSRAM). El desactivar estas opciones puede disminuir notablemente el rendimiento del sistema. Solo debe desactivarla como método de diagnóstico si tiene problemas de memoria y quiere comprobar si es la memoria Cache la causante de estos.

CPU L2 Cache ECC Checking.

Permite activar o no el chequeo de la memoria cache de segundo nivel de un Pentium II

Quick Power On Self Test.

Cuando está activado (enable) este campo aumenta la velocidad de ejecución de las rutinas del POST, ya que permite al procesador no realizar ciertos pasos de esta rutina, esto se refleja en un proceso de carga del sistema (Boot) mucho más rápido pero conspira contra un chequeo más profundo del hardware del sistema (incluido el correspondiente a la memoria). Es recomendable que normalmente tenga esta opción desactivada, ya que es mejor encontrar el problema durante el POST que perder los datos durante la operación normal.

HDD Sequence SCSI/IDE First.

Las computadoras actuales dan la posibilidad de conectar en su interior discos duros

de tecnologías diferentes como es el caso de los IDE y SCSI. Normalmente en un sistema AT el despertar del sistema se hace por el disco duro IDE, lo cual impide que se pueda cargar el sistema operativo desde un disco duro SCSI, el cual tiene su propio controlador y BIOS. Esta dificultad queda resuelta al tener la posibilidad en el SETUP, de definir por que tipo de disco desea se realice la carga del sistema.

Boot Sequence.

Este campo determina por donde la computadora realizará la carga del S.O. Los BIOS actuales no solo dan la facilidad de despertar por floppy o disco duro, permiten además cargar el S.O desde unidades poco comunes como pueden ser un lector de CDROM, una torre LS120 o un IOMEGA ZIP. En algunas versiones de los BIOS AWARD, dentro de esta opción (**Boot Sequence**) se incluye la anterior (**HDD Sequence SCSI/IDE First**). Los siguientes son valores frecuentes para esta opción.

A, C (Implicito)
C, A
C only
C, CDROM, A
CDROM, C, A
A, C, SCSI
C, A, SCSI
D, A, SCSI
E, A, SCSI
F, A, SCSI
SCSI, A, C
SCSI, C, A
LS120, C
LS/ZIP, C

Leyenda
C: IDE Master Primario
D: IDE Slave Primario
E: IDE Master Secundario
F: IDE Slave Secundario
LS: LS120
ZIP: IOMEGA ZIP Drive

Boot Up Floppy Seek.

Durante el POST, el BIOS determinará si la torre de floppy instalada es de 40 o 80 pistas. Las torres de 360 K son las únicas que tienen 40 pistas mientras que las otras (760K, 1.2M y 1.44M) son de 80 pistas. Esto lo hace emitiendo un comando de búsqueda (Seek) a la torre, que hace que la cabeza de la torre se mueva adelante y detrás.

No es recomendable tener esta opción activada, debido fundamentalmente a que consume tiempo durante la carga del sistema y además hace trabajar a la torre sin que exista normalmente un disco colocado en ella, lo cual puede afectar los

Elementos de Arquitectura y Seguridad Informática

mecanismos de la torre. En algunos sistemas es necesario tener esta opción activada para poder despertar por la torre de floppy, además de tener seleccionada a la torre "A" como primer dispositivo en la secuencia de carga (**Boot Sequence**).

Enabled (Implícito)	El BIOS interroga a la torre de floppy para determinar si es de 40 u 80 pistas. Note que el BIOS no puede diferenciar entre torres de 720K, 1.2M o 1.44M ya que todas tienen 80 pistas
Disabled	El BIOS no interrogará a la torre para determinar el número de pistas

Floppy Disk Access Control.

Se asigna protección para los ficheros que han sido copiados en las torres de floppy de su computadora.

R/W	Permite accesos de lectura y escritura a las torres.
Read Only	Sólo permite lecturas desde la torre de Floppy.

Swap Floppy Drive.

Permite intercambiar las letras de las torres de floppy sin necesidad de hacer el cambio físico en el cable. Por ejemplo si Ud. tiene dos torres de Floppy (A y B), y activa esta opción (Enable) le puede asignar a la primera torre la letra B y a la segunda la letra A. El valor implícito es desactivado (Disable).

Nota: Como este cambio se hace en el BIOS, sin afectar la definición de las torres de Floppy en la pantalla del STANDARD CMOS SETUP, algunos sistemas como los copiadores físicos de diskettes y el Windows 95 no reconocen este intercambio de las torres correctamente.

Boot Up Numlock Status.

Indica el estado del teclado numérico después de finalizada la carga del sistema.

On (Implícito)	Se activa el teclado numérico.
Off	Se activan las teclas del movimiento del cursor (flechas).

Boot Up System Speed.

Selecciona la velocidad del sistema, es decir a la que correrá el sistema inmediatamente después del encendido.

High	Fija la velocidad al máximo valor.
Low	Fija la velocidad al valor mínimo.

Typematic Rate Setting.

Este parámetro permite activar o desactivar la función de repetición del teclado. Cuando está activado, al mantener apretada una tecla este generará repetidamente los códigos de dicha tecla hasta que esta sea liberada.

Enabled	Activa la función de repetición
Disabled	Desactiva la función de repetición.

Typematic Rate (Chars/Sec).

Esta opción permite controlar la velocidad de repetición de los códigos de las teclas. Solo tiene validez si la opción **Typematic Rate Setting** está activada. Los valores posibles son los siguientes.

6	6 caracteres por segundo
8	8 caracteres por segundo
10	10 caracteres por segundo
12	12 caracteres por segundo
15	15 caracteres por segundo
20	20 caracteres por segundo
24	24 caracteres por segundo
30	30 caracteres por segundo

Typematic Delay (Msec).

Determina el tiempo de demora entre la emisión de dos códigos de la misma tecla cuando esta se mantiene continuamente apretada.

250	250 milisegundos.
500	500 milisegundos.
750	750 milisegundos.
1000	1000 milisegundos.

IDE HDD Block Mode Sectors (HDD MAX).

IDE HDD Block Mode (Enable, Disable).

Aumenta el rendimiento del disco duro haciendo una transferencia de múltiples sectores en vez de una transferencia de un solo sector. Esta opción también suele aparecer en la pantalla INTEGRATED PERIPHERALS.

Elementos de Arquitectura y Seguridad Informática

Enabled	Activa el modo bloque del disco duro IDE.
Disabled	Desactiva el modo bloque de disco duro IDE.
HDD MAX	Activa el modo bloque de disco duro IDE con el número máximo de bloques que soporta el disco.

Gate A20 Option.

La opción Gate A20 se refiere a la manera en que sistema direcciona la memoria por encima del primer megabyte (Memoria Extendida). Cuando se fija en Fast, el Chipset del sistema controla la señal del Bus **GateA20**. Cuando se fija en Normal, un terminal del controlador del teclado se encarga de este control (como en el diseño original de la AT). Cuando se fija en Fast se aumenta la velocidad del sistema considerablemente, particularmente con sistemas operativos como Windows y OS/2, que trabajan en modo protegido y hacen un uso extensivo de la Memoria Extendida.

Security Option.

Este campo permite seleccionar el nivel de seguridad que permitirá el Sistema para limitar el acceso de intrusos a su computadora mediante una contraseña de seguridad que se introduce en el Menú Principal. Tiene dos valores posibles:

System (Implícito)	El sistema no despertará o la entrada al SETUP será denegada si no se suministra la contraseña correcta.
Setup	El sistema despertará pero será denegada la entrada al SETUP si no se suministra la contraseña correcta.

PS/2 Mouse Function Control.

Controla la asignación de la IRQ 12 para un Mouse PS/2. El valor implícito AUTO activa IRQ12 cuando Ud. use un Mouse PS/2. Esta IRQ será reservada para otras tarjetas de expansión en el caso de que su Mouse sea serie.

PCI/VGA Palette Snoop.

Esta opción da la posibilidad (activada) de resolver los conflictos que se generan al instalar en la computadora dos tarjetas de video que usan las mismas direcciones de paleta (Palette Address) y que están conectadas al mismo tiempo en el Bus PCI. Tales como tarjetas de captura de video o MPEG. La tarjeta de video PCI VGA es "silenciada" mientras la tarjeta MPEG/Capturadora de Video funciona normalmente.

Al activar esta opción se le informa a la tarjeta de video PCI VGA que debe mantener silencio (y evitar así el conflicto) cuando el registro de paleta es actualizado, es decir, debe aceptar los datos sin emitir ninguna señal de confirmación.

OS/2 Onboard Memory –64 M. (Enable/Disable).

OS Select For Dram > 64MB (OS/2, Non-OS/2).

Active esta opción (Enable, OS/2) si utiliza el sistema operativo OS/2 con más de 64 MB de RAM. Si no déjelo desactivado (Disable, Non.OS/2) que es el valor implícito.

Video ROM BIOS Shadow.

Con la activación de esta opción es posible copiar el contenido la ROM del BIOS de VIDEO a la RAM, donde el acceso es mucho más rápido, puesto que puede ser leído de esta memoria a través un Bus de 32 bits lo cual permite un aumento de las prestaciones del sistema.

Nota: A la memoria RAM donde se copia el contenido de una memoria ROM, se le conoce como **Shadow RAM**. Normalmente en la PC este tipo de memoria ocupa las direcciones entre los primeros 640 KB y 1024KB.

C800- CBFF SHADOW

CC00- CFFF SHADOW

D000- D3FF SHADOW

D400- D7FF SHADOW

D800- DBFF SHADOW

DC00- DFFF SHADOW

Estas seis opciones son para hacer el "Shadow" del código de las memorias ROM que se pudieran encontrar sobre tarjetas de expansión y ocupando estas direcciones. Para esto es necesario conocer cuales son las direcciones de la ROM instalada sobre la tarjeta de expansión. Cuando hacemos el "Shadow" a la ROM se reduce la cantidad de memoria RAM disponible entre 640 KB y 1024 KB en la misma proporción de la cantidad usada para este propósito.

Nota: En versiones anteriores los segmentos correspondiente al código del BIOS (E000 y F000) se les hacia el "Shadow" activando la opción **System BIOS Shadow**, en los BIOS actuales esta área implícitamente, siempre se copia en memoria RAM, no solo para aumentar la velocidad de acceso al código del BIOS sino también para aprovechar al máximo la capacidad de la memoria FLASH ROM.

Opciones del Menú CHIPSET FEATURES SETUP.

Elementos de Arquitectura y Seguridad Informática

ROM PCI/ISA BIOS (2A41BS29) CHIPSET FEATURES SETUP AWARD SOFTWARE, INC.

Auto Configuration	: Disable	Onboard 496B IDE Port	: Both
ISA Bus Clock	: 7.159MHz	IDE 0 Master Mode	: Auto
LBD# Sample Point	: End of T3	IDE 0 Slave Mode	: Auto
		IDE 1 Master Mode	: Auto
		IDE 1 Slave Mode	: Auto
		Onboard FDD Controller	: Enabled
DRAM Speed	: Fastest	Onboard Serial Port 1	: COM1
DRAM Write Cycle	: 1 WS	Onboard Serial Port 2	: COM2
DRAM Write CAS Pulse	: 2 CCLK	Onboard Parallel Port	: 378H
		Onboard Parallel Mode	: EPP/SPP
		Serial Port 1 MIDI	: Disabled
		Serial Port 2 MIDI	: Disabled
CPU Burst Write	: Disable	ESC : Quit	!← : Select Item
L2 Cache Policy	: Write Back	F1 : Help	PU/PD/+/- : Modify
Cache Write Cycle	: 2 CCLK	F5 : Old Values (Shift)	F2 : Color
Cache Burst Read Cycle	: 1 CCLK	F7 : Load Setup Defaults	
L2 Cache/DRAM Cycle WS	: 2 CCLK		

Esta opción del menú principal incluye parámetros que dependen de las facilidades específicas que brinda el Chipset de la Tarjeta Madre y que están íntimamente relacionadas con el rendimiento del sistema. Entre estas facilidades se encuentran la administración del BUS y los accesos a los recursos de memoria, tales como la DRAM o la Cache Externa, también coordina la comunicación entre el BUS ISA convencional y el PCI, entre otras acciones. Algunas de estas Opciones o sus Valores pudieran no estar presente en todas las versiones del SETUP del BIOS AWARD.

Precaución: Asegúrese de que Ud. comprende completamente las opciones de este menú antes de tratar de modificar cualquiera de ellas. Ud. puede hacer cambios aquí que favorezcan el aumento de las prestaciones de su sistema. Sin embargo, esto puede causar que el sistema se vuelva inestable si la selección no es la correcta para la configuración de este. En caso de esto ocurra restablezca la configuración anterior o cargue los valores implícitos del SETUP.

Auto Configuración (Enable/Disable o 60ns/70ns)

Dram Timing (60ns/70ns).

Esta opción permite fijar la velocidad de trabajo de sus memorias. La velocidad especificada debe coincidir con la velocidad de la memoria instalada en su computadora. La configuración por defecto es de 60ns para la DRAM, si sus

memorias son de 70 ns esta configuración debe ser cambiada para 70 ns. Esto es sólo válido para los SIMM EDO o Fast Page, no para los DIMM SDRAM.

Cuando la opción de **Auto Configuración** tiene los valores Enable/Disable, se refiere a los valores que tomarán las opciones que configuran el atiemppamiento de la DRAM y la memoria Cache, los cuales se fijan en valores predeterminados de acuerdo al CPU instalado y al reloj del sistema. El desactivar esta opción (Disable) le permite especificar su propio atiemppamiento para la DRAM. Es muy recomendable dejar que sea el sistema el que lo configure de forma automática. En ocasiones cuando se habilita esta opción hay algunas opciones de este menú que no se pueden variar de forma manual.

Recomendación: Como regla general, en todas las opciones referidas a la memoria, trate de escoger siempre los valores menores y pruebe el funcionamiento de su computadora después de efectuar el cambio, fundamentalmente ejecute Windows 95 y varias aplicaciones para utilizar ampliamente la memoria. Si se presentan problemas o bloqueos del sistema escoja los valores implícitos del BIOS o el SETUP (F6 o F7) o seleccione un valor menor.

Fast RAS to CAS Delay.

EDO RAS# to CAS# Delay.

Se encuentran relacionada con el trabajo de la memoria, permite definir el tiempo de demora entre la señal RAS (Row Address Strobe) y la señal CAS (Column Address Strobe). Los valores posibles son 2 o 3 períodos de reloj. El implícito es 3.

DRAM Leadoff Timing.

“LeadOff” significa el atiemppamiento del primer ciclo de memoria en una lectura o escritura de ráfaga. Realmente este parámetro controla los valores para el atiemppamiento de la opción “**Page miss read/write Leadoff**”, los relojes de precarga del RAS y la demora entre el RAS y el CAS. Así los cuatro dígitos de los valores posibles que puede tener esta opción representan: Read Lead off /Write Lead off /RAS Precharge /RAS to CAS delay.

Los valores posibles son:

11/7/3/4

10/6/3/3

11/7/4/4

10/6/4/3

El valor implícito es 10/6/3/3 lo cual significa que tiene:

10/x/x/x DRAM Page miss Read.

6/x/x/x DRAM Page miss Write.

3 relojes de precarga del RAS.

Elementos de Arquitectura y Seguridad Informática

3 relojes de demora entre el RAS y el CAS.

DRAM RAS# Precharge Time.

La DRAM debe ser continuamente refrescada o se perderían los datos que ella almacena. Normalmente la DRAM es refrescada enteramente como resultado de un acceso simple. Esta opción permite determinar el número de relojes del CPU separados para que la señal RAS (Row Address Strobe) acumule carga antes de que la DRAM sea refrescada. Si el tiempo fijado es insuficiente, el refrescamiento estará incompleto y se perderán datos. Los valores posibles son 3 o 4 relojes.

Refresh Cycle Time.

Esta función fija el período de refrescamiento de la DRAM. Un valor bajo para el período del ciclo de refrescamiento permite incrementar el ancho de banda disponible para las transferencias de datos. Algunas DRAM no permiten un período de refrescamiento por debajo del implícito de 187.2 μ s. Los valores posibles son: ver **BIOS MB ASUS**.

DRAM RAS to CAS Delay.

Cuando la DRAM es refrescada, las filas y las columnas son direccionadas separadamente. Esta opción permite seleccionar el atiemppamiento de desde el RAS al CAS. Los valores posibles son una demora de 2 o 3 relojes del CPU.

DRAM Read Burst (EDO/FP).

Este parámetro ajusta los estados de espera de lectura entre la Cache L2 y la DRAM. Cada vez que el CPU no encuentra el dato en la Cache L2, él ejecuta cuatro ciclos continuos de memoria sobre cuatro direcciones continuas de memoria. Por tanto, hay cuatro valores que ajustar.

Read Burst significa la emisión de cuatro ciclos continuos de lectura de memoria sobre cuatro direcciones predefinidas de la DRAM. El valor implícito es x222/x333 para memorias DRAM EDO o FPM de 60 ns. Esto significa que el segundo, tercer y cuarto ciclo de memoria son de 2 relojes del CPU para la EDO y de 3 para la FPM. La x es el atiemppamiento del primer ciclo de memoria y depende del valor del "**DRAM Lead off Timing**". Mientras menor sea la combinación escogida, más rápido el sistema podrá direccionar la memoria. Los valores permitidos son:

EDO/FPM
x444/x444
x333/x444
x222/x333

DRAM Write Burst (EDO/FP).

Este parámetro ajusta los estados de espera de escritura entre la Cache L2 y la DRAM. El trabajo de la L2 se basa en una política de actualización de memoria principal Write-Back y cada proceso de escritura de la cache consiste en cuatro ciclos continuos de escritura de cache. Por tanto, hay cuatro valores que ajustar.

Write Burst significa la emisión de estos cuatro ciclos continuos de escritura de memoria sobre cuatro direcciones predefinidas de la DRAM. Este parámetro fija el valor del atiemppamiento de escritura de la DRAM para el segundo, tercer y cuarto ciclo de memoria. La x es el atiemppamiento del primer ciclo de memoria y depende del valor del "DRAM Lead off Timing". Los valores permitidos son los siguientes y no existen diferencias entre EDO y FP:

x444
x333
x222

Enhanced Page Mode.

Cuando está habilitado permite al BIOS del sistema predeterminedar si el próximo acceso a memoria está dentro o fuera de la misma página. Esto dirige el comienzo del tiempo de precarga, si está fuera de la página.

Linear Burst Mode

Linear Mode SRAM Suport.

Cuando se activa (enable) permite configurar el modo de escritura/lectura de datos desde el CPU a la DRAM. Si Ud. usa un CPU Cyrix (o IBM) active esta opción para lograr un ligero incremento en la transferencia de datos. Si Ud. usa un procesador Intel o AMD-K5, mantenga el valor implícito de desactivado ya que estos procesadores no soportan este modo.

Nota: En algunas Tarjetas, como la FIC VA-501, además hay que seleccionar correctamente un Jumper para escoger entre el Linear Burst Mode de los procesadores Cyrix e IBM y el Intel Burst Mode de los procesadores Intel y AMD-K5.

DRAM ECC/Parity Select.

Aquí se selecciona el tipo de chequeo de memoria que se realizará durante las operaciones de memoria.

Disable	No realiza ningún chequeo de memoria.
Parity	Hace el chequeo de paridad tradicional. Solo permite detectar errores en un bit.

Elementos de Arquitectura y Seguridad Informática

ECC	Implementa un nuevo método de chequeo y corrección de errores, que permite detectar errores en dos bits y corregirlos en uno. Es necesario contar con el chipset
------------	--

CPU Pipeline.

Cuando está activado permite que el CPU Pentium ejecute la función del Pipeline. El Pipeline en el CPU permite ir procesando varias instrucciones de forma casi paralela. Por esta razón, es conveniente dejar esta opción habilitada para no afectar el rendimiento del sistema.

16 bit ISA Wait State.

Establece la cantidad de estados de espera para las tarjetas de 16 bit ISA.

16/8 bit I/O Recovery Time.

Para algunos Chips de Entrada/Salida muy viejos, después de la ejecución de un comando de E/S, el dispositivo requiere de una cierta cantidad de tiempo (Recovery Time) antes de la ejecución del próximo comando. Esto es debido a que el CPU opera mucho más rápido que el BUS de E/S y debe esperar por el completamiento de esta operación antes recoger los resultados o emitir otro comando similar.

Dado que existe una nueva generación de CPU's y de Chipset's, la emisión de un comando de E/S es más rápida y en ocasiones el tiempo de recuperación es menor que el especificado para los dispositivos antiguos, esta opción le permite especificar la demora de un comando de E/S de 8 o 16 Bits en función de una cantidad de relojes del Bus ISA. Si Ud. encuentra que su tarjeta ISA de E/S de 8 (16) bits trabaja de forma inestable trate de extender el tiempo de recuperación por esta opción.

El valor implícito del BIOS para 8 bits es de 4 relojes ISA y de un reloj ISA para 16 bits. Si Ud. selecciona NA, el Chipset automáticamente insertará 3.5 relojes del sistema para ambos casos. Los valores posibles son:

8 Bits	16 bits
1	1
2	2
3	3
4	4
5	NA
6	
7	
8	
NA	

ISA BUS Clock.

Establece el reloj del Bus para tarjetas ISA, como una división del reloj del BUS PCI. Algunas tarjetas ISA pudieran trabajar de forma inestable si este parámetro tiene un

valor incorrecto, trate de variarlo para resolver estos problemas. Los valores permitidos son:

PCICLK/4
PCICLK/3

Video BIOS/System BIOS Cacheable.

Cuando se habilitan estas opciones permiten que las direcciones del BIOS de Video (C0000H-C7FFFH) y el BIOS del Sistema (F0000H-FFFFFH) sean "Cacheadas", es decir, que los códigos de programa que contienen se ejecuten desde las memorias SRAM que componen la memoria cache, en vez de ejecutarlos desde memorias ROM o DRAM (si está habilitada la "Shadow RAM") que son más lentas. Esto permitirá una mayor rapidez de ejecución de dichos códigos.

Memory Hole AT 15M-16M

Esta opción permite reservar espacios de direcciones de memoria para un tipo especial de tarjeta de expansión ISA, que requiere de esta configuración. Normalmente son tarjetas que trabajen directamente con la memoria usando una técnica de mapeo de memoria de E/S a través del Bus ISA directamente.

Esto provoca que a partir de memoria especificada (15M) y en lo adelante, esta zona sea transparente para el sistema y no pueda ser utilizada por el sistema operativo. Si Ud. no tiene una tarjeta de este tipo deje esta opción desactivada porque podría "Perder" toda la memoria por encima de los 15 MB.

Delayed Transaction.

PCI Delayed Transaction.

Permite cuando se activa (enable) que se libere el Bus PCI durante los accesos de la CPU a las tarjetas ISA de 8 Bit. Lo cual consume cerca de 50 o 60 relojes del Bus PCI si no está activa esta opción. Desactívelo para algunos controladores PCI e ISA que no cumplen con la versión PCI 2.1. De forma general trate de activarlo o desactivarlo si tiene algún problema con tarjetas ISA.

On board VGA Memory Size.

Permite establecer 1MB, 2MB o 4 MB de memoria para el controlador de vídeo integrado en la tarjeta madre ASUS SP97-V. Mayor cantidad de memoria permitirá una mayor cantidad de colores y resolución, pero disminuirá la Memoria Extendida del sistema.

Onboard VGA Memory Clock.

Esta función permite que al usuario la selección de la velocidad de la tarjeta de vídeo, definiendo 50 Mhz para modo normal, 60 Mhz para rápido y 66 Mhz reservado para muy rápido. Si su monitor mostrase información que no puede reconocer, **se debe** bajar la velocidad para sincronizarla con el rango de frecuencia del monitor.

Opciones del Menú Power Management SETUP.

Esta opción permite configurar efectivamente el modo de ahorro de energía con el objetivo de reducir el consumo de potencia de su equipo, dando la posibilidad de apagar el monitor y desconectar el disco duro después de un periodo de inactividad. En ocasiones esta Pantalla tiene varias secciones separadas, entre estas se encuentran:

PM Timers: Controla los tiempos para que se activen los modos de ahorro de energía, los campos incluidos en esta sección son "HDD Power Down", la cual pone al disco duro en el modo de más bajo consumo de energía los modos de inactivación del sistema **Doze**, **Standby** y **Suspend**.

PM Events: Esta sección controla los eventos que despertarán al sistema. Si se detecta actividad en cualquiera de estas IRQ's, el sistema despertará del modo de inactivación en que se encuentre.

Power Management.

Esta opción actúa como el control maestro para los modos de ahorro de potencia. Permite seleccionar el tipo (o grado) de ahorro de energía y está directamente relacionado con los tiempos de activación que tomarán los siguientes modos: Doze Mode, Standby Mode, Suspend Mode y HDD Power Down.

Existen cuatro posibles selecciones para **Power Management**, tres de las cuales ya tienen valores fijos.

Max Saving.	Inicializa y predetermina los temporizadores en sus valores máximos.
Min Saving.	Inicializa y predetermina los temporizadores en sus valores mínimos.
User Defined.	Permite configurar manualmente los valores de las opciones del ahorro de energía.
Disable.	Desactiva totalmente las facilidades del ahorro de energía.

	Doze	Standby	Suspend	HDD Power Down
Min Saving	1 hora	1 hora	1 hora	15 minutos
Max Saving	1 Minuto	1 Minuto	1 Minuto	1 Minuto

Los modos se activan sucesivamente en este mismo orden.

PM Control By APM.

Activando esta opción (Yes), es posible utilizar un controlador APM (Advanced Power Management, o Administrador avanzado de la Potencia) para ampliar las posibilidades del modo Max Saving y detener el reloj interno del CPU. Si se desactiva esta opción (No), el BIOS ignora las especificaciones del APM, solo debe hacerlo si planea no usar el modo Max Saving.

Nota: El APM debe ser instalado con el Sistema Operativo. Para ambiente DOS, necesita agregar la siguiente línea al CONFIG.SYS: DEVICE = C:\DOS\POWER.EXE. Para Windows 3.x y Windows 95, necesita instalarlos con la facilidad de APM. En el panel de control aparecerá un icono con una batería y un cable de alimentación y la etiqueta Power (Energía), indicando que el APM está instalado. Dando doble Click sobre este icono le permite variar las posibilidades de ahorro de energía que ofrece Windows.

Video OFF Option.

Video OFF After.

Esta opción determina cuando se debe activar el apagado del monitor, es decir en que modo de ahorro de energía. Las posibilidades son:

Doze => Off	Lo apaga cuando el sistema entra en el modo Doze.
Susp,Stby => Off	Lo apaga cuando el sistema entra en el modo Suspend o Standby.
Suspend => Off	Lo apaga cuando el sistema entra en el modo Suspend.
All Modes Off	Lo apaga si el sistema entra en el modo Doze, Standby o Suspend.
Always On (NA)	Siempre encendido, independientemente del modo activo.

Video OFF Method.

Aquí se determina la manera en que se apaga el monitor. Existen varias formas, las cuales se explican en la siguiente tabla. Es importante resaltar que el CRT (Monitor) es el dispositivo que consume mayor cantidad de potencia (algunos cientos de Watts o menos en dependencia de las características de este). Para realmente ahorrar energía es necesario apagarlo cuando no esté en uso. Los Monitores Green (también conocidos como Energy Star Monitors) ayudan a reducir el consumo de potencia en un 90% sin tener que apagarlo realmente.

Blank Screen	Limpia la pantalla del monitor escribiendo espacios en blanco en la memoria de video.
V/H SYNC + Blank	Además de limpiar la pantalla, desconecta las señales V-SYNC y H-SYNC emitidas por la tarjeta de video hacia el monitor. Los monitores Green detectan estas señales para apagar el cañón de electrones del CRT.

Elementos de Arquitectura y Seguridad Informática

DPMS	Seleccione esta opción si su monitor y tarjeta de video soportan el estándar VESA DPMS (Display Power Management Signaling). Use el programa suministrado por la tarjeta de video para seleccionar los valores de ahorro de energía para el monitor.
-------------	---

Para lograr un buen funcionamiento de este sistema se debe seleccionar el método de apagado V/H Sync + Blank o el DPMS, ya que estos garantizan un apagado efectivo del monitor. El Método Blank Screen solamente apaga la pantalla, pero el equipo sigue consumiendo el 100 % de la energía.

Algunos Refrescadores de pantallas (Screesavers) son programas que están corriendo y obviamente no existirá período de inactividad del CPU y en ocasiones ni para el HDD, por tanto las opciones standard del BIOS podrían no apagar nunca su monitor ni entrar en los modos de ahorro de energía. Es recomendable no usar refrescadores muy complejos o compruebe prácticamente que estos no interrumpen el funcionamiento normal del administrador de ahorro de energía. Los que trae el Windows 95 funcionan correctamente y no existe ningún conflicto. De todas formas la mejor manera de proteger su tubo de pantalla y ahorrar energía es desconectando temporalmente el monitor usando las posibilidades que le ofrece el BIOS y el Windows 95.

Modem Use IRQ.

Aquí se selecciona la línea de interrupción (IRQ) usada por el modem del sistema, si lo hubiera. Cualquier actividad sobre esta IRQ siempre provocaría que el sistema se despierte. Los valores posibles son NA, 3 (implícito), 4, 5, 7, 9, 10, 11.

Suspend Switch Enable.

Este campo activa o desactiva el conector SMI sobre la tarjeta madre, a este conector se conecta el interruptor Suspend que se encuentra en el panel delantero de la computadora. Este interruptor permite que manualmente se obligue a la computadora a entrar en el modo **Suspend** de ahorro de energía. Esto solo es posible si esta opción y la del **Power Management** están activadas.

Sección PM Timers.

HDD Off After.

HDD Power Down.

HDD Power Management.

Permite especificar el tiempo que puede permanecer inactivo el HDD antes de entrar en el modo de ahorro de energía. En este caso se detiene el movimiento del motor del disco. Esta opción no afecta los HDD SCSI. Los valores posibles son: **Desactivado** y desde **1 minuto** hasta **15 minutos** de inactividad. En este caso esta opción es independiente de cualquiera de los otros modos de ahorro de energía (Doze, Standby, Suspend) , sin embargo en algunos BIOS existe la Opción **When**

Suspend, donde se detendrá el motor del HDD cuando se entre en el modo Suspend. Cuando el HDD está en el modo de ahorro de energía cualquier acceso al disco lo despertará.

Doze Mode.

Esta opción permite fijar el período de tiempo de inactividad después del cual el sistema entra en el modo Doze. En este modo, se baja la frecuencia del reloj del CPU, El rango en el cual se baja esta frecuencia es especificado en la opción "**Throttle Duty Cycle**", la cual es bastante poco común que aparezca. Cualquier actividad que se detecte devuelve el sistema a su máxima potencia. La actividad (o eventos) del sistema se detectan a través del monitoreo de las IRQ's. Los valores posibles oscilan entre 1 minuto y una hora o desactivado.

Standby Mode.

Esta opción permite fijar el período de tiempo de inactividad después del cual el sistema entra en el modo Standby. En este modo, se baja la frecuencia del reloj del CPU, el disco duro podría apagarse y se activan los modos de ahorro de energía del monitor. Cualquier actividad que se detecte devuelve el sistema a su máxima potencia. La actividad (o eventos) del sistema se detectan a través del monitoreo de las IRQ's. Los valores posibles oscilan entre 1 minuto y una hora o desactivado.

Suspend Mode.

Esta opción permite fijar el período de tiempo de inactividad después del cual el sistema entra en el modo Suspend. En este modo, se detiene la frecuencia del reloj del CPU y se detienen todos los demás dispositivos. Cualquier actividad que se detecte devuelve el sistema a su máxima potencia. La actividad (o eventos) del sistema se detectan a través del monitoreo de las IRQ's. Los valores posibles oscilan entre 1 minuto y una hora o desactivado.

En las tarjetas madres más modernas, que soportan las nuevas facilidades de administración de potencia que plantea el standard **ACPI (Advanced Configuration Power Interface)**, al transcurrir el tiempo especificado por esta, el modo **Suspend** puede tener dos posibilidades, la primera, **Power On Suspend** y la segunda **Suspend to hard Drive**. Cual de estas posibilidades usará el sistema cuando entre en el modo **Suspend** se escoge en la Opción "**Suspend Mode Option**".

ACPI es una especificación surgida en 1997 (PC97) y trata de ahorrar más energía mediante el control de la administración de la potencia a través del Sistema Operativo y no a través del BIOS. Debido a esto el Chipset debe suministrar una interface de registros estándar al S.O. para que este pueda apagar y encender diferentes partes del Chip o del sistema. La parte más atractiva del **ACPI** es la facilidad "**On Now**" la cual permite continuar su trabajo original sin necesidad de esperar que la máquina despierte, cargue Windows 95 y correr Winword. El Chipset TX de Intel soporta el ACPI.

Suspend Mode Option.

Elementos de Arquitectura y Seguridad Informática

Aquí se seleccionan las acciones que tomará el modo Suspend. Las posibilidades son:

Power On Suspend: Es el modo tradicional del modo **Suspend** de las Green PC, se detiene el reloj del CPU, se apagan todos los demás dispositivos pero se mantiene encendido el sistema hasta que se detecta alguna actividad en el teclado, mouse o el modem, en cuyo caso se devuelve el sistema a su máxima potencia. La actividad (o eventos) del sistema se detecta a través del monitoreo de las IRQ's.

Suspend to hard Drive: En este caso se salva el estado del sistema, contenido de la memoria y la imagen en pantalla hacia el disco duro y después se apaga totalmente el sistema. La próxima vez que se encienda el equipo, el sistema se carga, en pocos segundos, justo en lugar donde mismo estaba en el momento en que se suspendió.

Nota: Por el momento esto solo lo soportan unas pocas tarjetas y es necesario ejecutar determinados programas que garanticen el buen funcionamiento de este sistema.

Throttle Duty Cycle.

Clock Throttle ("Estrangular el ciclo del reloj", Perdonen la traducción) significa que en el estado de Doze o Standby el conteo de los relojes de CPU se reducen durante un tiempo determinado (no su frecuencia) en el rango especificado en este parámetro. Realmente el período por pulso de reloj del CPU no cambia. Por ejemplo, para un reloj del CPU de 66 Mhz, este sigue teniendo 30 ns de período de reloj aún cuando el sistema entre en alguno de estos modos.

El Chipset genera la señal STPCLK (Stop Clock) periódicamente para evitar que el CPU acepte el reloj desde el generador de reloj. Para la máxima potencia el CPU recibirá 66 M conteos en un segundo. Si la razón de demora del reloj es del 50 % el CPU solo recibirá 33 M pulsos en un segundo. Esto efectivamente reduce la velocidad del CPU así como su consumo de potencia.

Los valores posibles son 12.5 %, 25.0 %, 37.5 %, 50.0 %, 62.5 %, 75.5 %, 87.5 %.

Sección PM EVENTS/ Wake Up Events in Doze & Standby.

IRQ 3 (Wake Up Event).

IRQ 4 (Wake Up Event).

IRQ 8 (Wake Up Event).

IRQ 12 (Wake Up Event)

Los valores posibles para estas opciones son **ON**, se monitorea actividad de esta IRQ para despertar al sistema desde cualquier modo de ahorro de energía u **OFF** donde no se detecta actividad de estas IRQ's.

Sección Power Down Activities & Resume Events.

Seleccionando **ON** en cualquiera de las siguientes interrupciones se arrancaran los temporizadores del Administrador de Potencia cuando no se detecte actividad en el puerto de E/S o en el componente especificado. Si se selecciona **OFF** el BIOS no entrará en ninguno de los Modos de ahorro de energía cuando no se detecte actividad en la IRQ seleccionada. Las líneas de interrupciones que se pueden configurar son:

IRQ 3 (COM2)
IRQ 4 (COM1)
IRQ 5 (LPT2)
IRQ 6 (Floppy Disk)
IRQ 7 (LPT1)
IRQ 8 (Alarma del RTC)
IRQ 9 (IRQ 2 Rdir)
IRQ 10 (Reservada)
IRQ 11 (Reservada)
IRQ 12 (Mouse PS/2)
IRQ 13 (Coprocesador)
IRQ 14 (Disco duro)
IRQ 15 (Reservada)

Opciones del Menú Power Management SETUP.

ROM PCI/ISA BIOS (2A41BS29)
POWER MANAGEMENT SETUP
AWARD SOFTWARE, INC.

Power Management : Disable	IRQ3 (COM 2) : Enable
PM Control by APM : Yes	IRQ4 (COM, 1) : Enable
Video Off Method : V/H SYNC+Blank	IRQ5 (LPT 2) : Enable
Suspend Switch : Enable	IRQ6 (Floppy Disk): Enable
	IRQ7 (LPT 1) : Enable
** PM Timers **	IRQ8 (RTC Alarm) : Disable
HDD Off After : Disable	IRQ9 (IRQ2 Redir) : Enable
Doze Mode : Disable	IRQ10 (Reserved) : Enable
Standby Mode : Disable	IRQ11 (Reserved) : Enable
Suspend Mode : Disable	IRQ12 (PS/2 Mouse) : Enable
	IRQ13 (Coprocessor): Enable
** PM Events **	IRQ14 (Hard Disk) : Enable
PCI Master Activity: Enable	IRQ15 (Reserved) : Enable
COM Ports Activity : Enable	
LPT Ports Activity : Enable	
HDD Ports Activity : Enable	
DMA Ports Activity : Enable	
VGA Activity : Disable	
	ESC : Quit F10 : Select Item
	F1 : Help PU/PD/+/- : Modify
	F5 : Old Values (Shift)F2 : Color
	F7 : Load Setup Defaults

Esta opción permite configurar efectivamente el modo de ahorro de energía con el objetivo de reducir el consumo de potencia de su equipo, dando la posibilidad de

Elementos de Arquitectura y Seguridad Informática

apagar el monitor y desconectar el disco duro después de un periodo de inactividad. En ocasiones esta Pantalla tiene varias secciones separadas, entre estas se encuentran:

PM Timers: Controla los tiempos para que se activen los modos de ahorro de energía, los campos incluidos en esta sección son **"HDD Power Down"**, la cual pone al disco duro en el modo de más bajo consumo de energía los modos de inactivación del sistema **Doze**, **Standby** y **Suspend**.

PM Events: Esta sección controla los eventos que despertarán al sistema. Si se detecta actividad en cualquiera de estas IRQ's, el sistema despertará del modo de inactivación en que se encuentre.

Power Management.

Esta opción actúa como el control maestro para los modos de ahorro de potencia. Permite seleccionar el tipo (o grado) de ahorro de energía y está directamente relacionado con los tiempos de activación que tomarán los siguientes modos: Doze Mode, Standby Mode, Suspend Mode y HDD Power Down.

Existen cuatro posibles selecciones para **Power Management**, tres de las cuales ya tienen valores fijos.

Max Saving.	Inicializa y predetermina los temporizadores en sus valores máximos.
Min Saving.	Inicializa y predetermina los temporizadores en sus valores mínimos.
User Defined.	Permite configurar manualmente los valores de las opciones del ahorro de energía.
Disable.	Desactiva totalmente las facilidades del ahorro de energía.

	Doze	Standby	Suspend	HDD Power Down
Min Saving	1 hora	1 hora	1 hora	15 minutos
Max Saving	1 Minuto	1 Minuto	1 Minuto	1 Minuto
Los modos se activan sucesivamente en este mismo orden.				

PM Control By APM.

Activando esta opción (**Yes**), es posible utilizar un controlador **APM** (Advanced Power Management, o Administrador avanzado de la Potencia) para ampliar las posibilidades del modo **Max Saving** y detener el reloj interno del CPU. Si se

desactiva esta opción (**No**), el BIOS ignora las especificaciones del **APM**, solo debe hacerlo si planea no usar el modo **Max Saving**.

Nota: El APM debe ser instalado con el Sistema Operativo. Para ambiente DOS, necesita agregar la siguiente línea al CONFIG.SYS: `DEVICE = C:\DOS\POWER.EXE`. Para Windows 3.x y Windows 95, necesita instalarlos con la facilidad de APM. En el panel de control aparecerá un icono con una batería y un cable de alimentación y la etiqueta **Power** (Energía), indicando que el APM está instalado. Dando doble Click sobre este icono le permite variar las posibilidades de ahorro de energía que ofrece Windows.

Video OFF Option.

Video OFF After

Esta opción determina cuando se debe activar el apagado del monitor, es decir en que modo de ahorro de energía. Las posibilidades son:

Doze => Off	Lo apaga cuando el sistema entra en el modo Doze.
Susp,Stby => Off	Lo apaga cuando el sistema entra en el modo Suspend o Standby.
Suspend => Off	Lo apaga cuando el sistema entra en el modo Suspend.
All Modes Off	Lo apaga si el sistema entra en el modo Doze, Standby o Suspend.
Always On (NA)	Siempre encendido, independientemente del modo activo.

Video OFF Method.

Aquí se determina la manera en que se apaga el monitor. Existen varias formas, las cuales se explican en la siguiente tabla. Es importante resaltar que el CRT (Monitor) es el dispositivo que consume mayor cantidad de potencia (algunos cientos de Watts o menos en dependencia de las características de este). Para realmente ahorrar energía es necesario apagarlo cuando no esté en uso. Los Monitores Green (también conocidos como Energy Star Monitors) ayudan a reducir el consumo de potencia en un 90% sin tener que apagarlo realmente.

Blank Screen	Limpia la pantalla del monitor escribiendo espacios en blanco en la memoria de video.
V/H SYNC + Blank	Además de limpiar la pantalla, desconecta las señales V-SYNC y H-SYNC emitidas por la tarjeta de video hacia el monitor. Los monitores Green detectan estas señales para apagar el cañón de electrones del CRT.
DPMS	Seleccione esta opción si su monitor y tarjeta de video soportan el estándar VESA DPMS (Display Power Management Signaling). Use el programa suministrado por la tarjeta de video para seleccionar los valores de ahorro de energía para el monitor.

Elementos de Arquitectura y Seguridad Informática

Para lograr un buen funcionamiento de este sistema se debe seleccionar el método de apagado V/H Sync + Blank o el DPMS, ya que estos garantizan un apagado efectivo del monitor. El Método Blank Screen solamente apaga la pantalla, pero el equipo sigue consumiendo el 100 % de la energía.

Algunos Refrescadores de pantallas (Screesavers) son programas que están corriendo y obviamente no existirá período de inactividad del CPU y en ocasiones ni para el HDD, por tanto las opciones standard del BIOS podrían no apagar nunca su monitor ni entrar en los modos de ahorro de energía. Es recomendable no usar refrescadores muy complejos o compruebe prácticamente que estos no interrumpen el funcionamiento normal del administrador de ahorro de energía. Los que trae el Windows 95 funcionan correctamente y no existe ningún conflicto. De todas formas la mejor manera de proteger su tubo de pantalla y ahorrar energía es desconectando temporalmente el monitor usando las posibilidades que le ofrece el BIOS y el Windows 95.

Modem Use IRQ.

Aquí se selecciona la línea de interrupción (IRQ) usada por el modem del sistema, si lo hubiera. Cualquier actividad sobre esta IRQ siempre provocaría que el sistema se despierte. Los valores posibles son NA, 3 (implícito), 4, 5, 7, 9, 10, 11.

Suspend Switch Enable.

Este campo activa o desactiva el conector SMI sobre la tarjeta madre, a este conector se conecta el interruptor Suspend que se encuentra en el panel delantero de la computadora. Este interruptor permite que manualmente se obligue a la computadora a entrar en el modo **Suspend** de ahorro de energía. Esto solo es posible si esta opción y la del **Power Management** están activadas.

Sección PM Timers.

HDD Off After.

HDD Power Down.

HDD Power Management.

Permite especificar el tiempo que puede permanecer inactivo el HDD antes de entrar en el modo de ahorro de energía. En este caso se detiene el movimiento del motor del disco. Esta opción no afecta los HDD SCSI. Los valores posibles son: **Desactivado** y desde **1 minuto** hasta **15 minutos** de inactividad. En este caso esta opción es independiente de cualquiera de los otros modos de ahorro de energía (Doze, Standby, Suspend) , sin embargo en algunos BIOS existe la Opción **When Suspend**, donde se detendrá el motor del HDD cuando se entre en el modo Suspend. Cuando el HDD está en el modo de ahorro de energía cualquier acceso al disco lo despertará.

Doze Mode.

Esta opción permite fijar el período de tiempo de inactividad después del cual el sistema entra en el modo Doze. En este modo, se baja la frecuencia del reloj del CPU, El rango en el cual se baja esta frecuencia es especificado en la opción "**Throttle Duty Cycle**", la cual es bastante poco común que aparezca. Cualquier actividad que se detecte devuelve el sistema a su máxima potencia. La actividad (o eventos) del sistema se detectan a través del monitoreo de las IRQ's. Los valores posibles oscilan entre 1 minuto y una hora o desactivado.

Standby Mode.

Esta opción permite fijar el período de tiempo de inactividad después del cual el sistema entra en el modo Standby. En este modo, se baja la frecuencia del reloj del CPU, el disco duro podría apagarse y se activan los modos de ahorro de energía del monitor. Cualquier actividad que se detecte devuelve el sistema a su máxima potencia. La actividad (o eventos) del sistema se detectan a través del monitoreo de las IRQ's. Los valores posibles oscilan entre 1 minuto y una hora o desactivado.

Suspend Mode.

Esta opción permite fijar el período de tiempo de inactividad después del cual el sistema entra en el modo Suspend. En este modo, se detiene la frecuencia del reloj del CPU y se detienen todos los demás dispositivos. Cualquier actividad que se detecte devuelve el sistema a su máxima potencia. La actividad (o eventos) del sistema se detectan a través del monitoreo de las IRQ's. Los valores posibles oscilan entre 1 minuto y una hora o desactivado.

En las tarjetas madres más modernas, que soportan las nuevas facilidades de administración de potencia que plantea el standard **ACPI** (Advanced Configuration Power Interface), al transcurrir el tiempo especificado por esta, el modo **Suspend** puede tener dos posibilidades, la primera, **Power On Suspend** y la segunda **Suspend to hard Drive**. Cual de estas posibilidades usará el sistema cuando entre en el modo **Suspend** se escoge en la Opción "**Suspend Mode Option**".

ACPI es una especificación surgida en 1997 (PC97) y trata de ahorrar más energía mediante el control de la administración de la potencia a través del Sistema Operativo y no a través del BIOS. Debido a esto el Chipset debe suministrar una interface de registros estándar al S.O. para que este pueda apagar y encender diferentes partes del Chip o del sistema. La parte más atractiva del **ACPI** es la facilidad "**On Now**" la cual permite continuar su trabajo original sin necesidad de esperar que la máquina despierte, cargue Windows 95 y correr Winword. El Chipset TX de Intel soporta el **ACPI**.

Suspend Mode Option.

Aquí se seleccionan las acciones que tomará el modo Suspend. Las posibilidades son:

Power On Suspend: Es el modo tradicional del modo **Suspend** de las Green PC, se detiene el reloj del CPU, se apagan todos los demás dispositivos pero se mantiene

Elementos de Arquitectura y Seguridad Informática

encendido el sistema hasta que se detecta alguna actividad en el teclado, mouse o el modem, en cuyo caso se devuelve el sistema a su máxima potencia. La actividad (o eventos) del sistema se detecta a través del monitoreo de las IRQ's.

Suspend to hard Drive: En este caso se salva el estado del sistema, contenido de la memoria y la imagen en pantalla hacia el disco duro y después se apaga totalmente el sistema. La próxima vez que se encienda el equipo, el sistema se carga, en pocos segundos, justo en lugar donde mismo estaba en el momento en que se suspendió.

Nota: Por el momento esto solo lo soportan unas pocas tarjetas y es necesario ejecutar determinados programas que garanticen el buen funcionamiento de este sistema.

Throttle Duty Cycle.

Clock Throttle ("Estrangular el ciclo del reloj", Perdonen la traducción) significa que en el estado de Doze o Standby el conteo de los relojes de CPU se reducen durante un tiempo determinado (no su frecuencia) en el rango especificado en este parámetro. Realmente el período por pulso de reloj del CPU no cambia. Por ejemplo, para un reloj del CPU de 66 Mhz, este sigue teniendo 30 ns de período de reloj aún cuando el sistema entre en alguno de estos modos.

El Chipset genera la señal STPCLK (Stop Clock) periódicamente para evitar que el CPU acepte el reloj desde el generador de reloj. Para la máxima potencia el CPU recibirá 66 M conteos en un segundo. Si la razón de demora del reloj es del 50 % el CPU solo recibirá 33 M pulsos en un segundo. Esto efectivamente reduce la velocidad del CPU así como su consumo de potencia.

Los valores posibles son 12.5 %, 25.0 %, 37.5 %, 50.0 %, 62.5 %, 75.5 %, 87.5 %.

Sección PM EVENTS/ Wake Up Events in Doze & Standby.

IRQ 3 (Wake Up Event).

IRQ 4 (Wake Up Event).

IRQ 8 (Wake Up Event).

IRQ 12 (Wake Up Event)

Los valores posibles para estas opciones son **ON**, se monitorea actividad de esta IRQ para despertar al sistema desde cualquier modo de ahorro de energía u **OFF** donde no se detecta actividad de estas IRQ's.

Sección Power Down Activities & Resume Events.

Seleccionando **ON** en cualquiera de las siguientes interrupciones se arrancaran los temporizadores del Administrador de Potencia cuando no se detecte actividad en el puerto de E/S o en el componente especificado. Si se selecciona **OFF** el BIOS no entrará en ninguno de los Modos de ahorro de energía cuando no se detecte

actividad en la IRQ seleccionada. Las líneas de interrupciones que se pueden configurar son:

IRQ 3 (COM2)
IRQ 4 (COM1)
IRQ 5 (LPT2)
IRQ 6 (Floppy Disk)
IRQ 7 (LPT1)
IRQ 8 (Alarma del RTC)
IRQ 9 (IRQ 2 Rdir)
IRQ 10 (Reservada)
IRQ 11 (Reservada)
IRQ 12 (Mouse PS/2)
IRQ 13 (Coprocesador)
IRQ 14 (Disco duro)
IRQ 15 (Reservada)

. Opciones del Menú PnP AND PCI SETUP.

En esta sección se describe la configuración del Bus PCI del Sistema. PCI, o **Peripheral Component Interconnect**, es un tipo de Bus que permite a los dispositivos de Entrada/Salida operar a una velocidad cercana a la que el CPU usa cuando se comunica con otros dispositivos del sistema. Esta sección cubre algunos aspectos muy técnicos y se recomienda que solo personas con experiencia deben cambiar los valores implícitos.

Resources Controlled By.

Si fija esta opción en **Auto**, el BIOS automáticamente configura todos los recursos del sistema. Si existieran conflictos o Ud. no está satisfecho con esta configuración puede, seleccionando el valor **Manual**, configurar de forma manual los recursos del sistema, (las líneas de interrupción y los canales de DMA).

PnP OS Installed.

Normalmente los recursos PnP son distribuidos por el BIOS durante el POST. Si Ud. está usando un sistema operativo PnP, como Windows 95, active este valor (**Yes**) para informarle al BIOS que configure solo los recursos necesarios para despertar el sistema (Tarjeta VGA, IDE o SCSI). El resto de los recursos del sistema serán distribuidos por el Sistema Operativo PnP, ya que este tiene la propiedad de detectar de forma automática los dispositivos que se instalen sobre su sistema y tengan también esta característica.

Reset Configuration data.

Habilite esta opción, sólo en el caso de que ocurra un conflicto después de que Ud. asigne de forma manual las IRQ o después de configurar el sistema. Esto permite que el sistema automáticamente limpie los datos de la última configuración y reasigne las líneas de interrupción (IRQ), los canales de DMA y las direcciones de Entrada/Salida con los valores implícitos del BIOS. Despierte nuevamente el sistema

Elementos de Arquitectura y Seguridad Informática

y desactive esta opción, para intentar configurar el sistema nuevamente o cuando ya lo tiene configurado sin conflictos.

IRQ x (3, 4, 5, 7, 9, 10, 11, 12, 13, 14, 15), (Legacy ISA, PCI/ISA PnP)

IRQ x Used By ISA (3, 4, 5, 7, 9, 10, 11, 12, 13, 14, 15), (Yes, No/ICU)

Escoja el valor **Legacy ISA (o Yes)** a una de estas opciones si Ud. instala una tarjeta de este tipo, es decir, que no es compatible con PnP y requiere que se seleccione una IRQ para su funcionamiento. Esto informa al BIOS PnP que debe reservar esa IRQ para una tarjeta ISA. El valor implícito es **PCI/ISA PnP (o No/ICU)**, lo cual indica que será el BIOS PnP quien distribuirá los recursos. Tenga en cuenta que las tarjetas PCI son siempre compatibles PnP, excepto las muy antiguas.

Nota: ICU significa **ISA Configuration Utility**, y es un utilitario que permite determinar si la tarjeta ISA está usando determinados recursos (IRQ, Canal DMA o espacio de memoria).

DMA x (0, 1, 3, 5, 6, 7).

Escoja el valor **Legacy ISA** a una de estas opciones si Ud. instala una tarjeta de este tipo, es decir, que no es compatible con PnP y requiere que se seleccione un canal de DMA para su funcionamiento. Esto informa al BIOS PnP que debe reservar ese canal para una tarjeta ISA. El valor implícito es **PCI/ISA PnP**. Tenga en cuenta que las tarjetas PCI no requieren canal DMA.

PCI IDE IRQ Map To.

Algunas tarjetas de expansión IDE PCI, muy antiguas, no son completamente compatibles con el PnP. Estas tarjetas requieren que se les especifique en que ranura (Slot) están conectadas para que el BIOS pueda configurar los recursos PnP correctamente. Esta opción permite seleccionar cualquier ranura PCI para una tarjeta IDE PCI. La opción **Auto** permite al BIOS configurar automáticamente las tarjetas IDE PCI instaladas. Este tipo de tarjeta no debe confundirse con los canales IDE integrados y es recomendable dejar esta opción en Auto, aún cuando no tengamos ninguna tarjeta de este tipo.

Los valores posibles son:

ISA
PCI-Slot1
PCI-Slot2
PCI-Slot3
PCI-Slot4
PCI-Auto

Primary IDE INT#.

Secondary IDE INT#.

Estas dos opciones, junto con "PCI IDE IRQ map to", especifican el enrutamiento de la IRQ para el Canal Primario o Secundario de la tarjeta de expansión PCI IDE (no de los canales IDE integrados). Ud. debe especificar el Slot usado por la tarjeta en la opción "PCI IDE IRQ Map To" y fijar la interrupción PCI (INTx) aquí, de acuerdo a la conexión de la interrupción sobre la tarjeta. Los valores posibles son A, B, C, D.

Slot 1 Using INT#.

Slot 2 Using INT#.

Slot 3 Using INT#.

Slot 4 Using INT#.

Algunos dispositivos PCI usan la señal de interrupción para indicar que necesitan el Bus PCI, Cada Ranura PCI es capaz de activar hasta cuatro interrupciones, INT#A, INT#B, INT#C, INT#D. **Implicítamente todos los Slots PCI usan la INT#A.**

Asignar la INT#B no tiene significado a menos que el dispositivo en el Slot requiera dos servicios de interrupción, en vez de solo una. De igual forma seleccionar INT#C significa que el dispositivo requiere tres interrupciones y similarmente para INT#D. Las interrupciones de cada ranura PCI están alineadas como se muestra en la tabla siguiente.

Slot PCI	Localización 1 (Pin A6)	Localización 2 (Pin B7)	Localización 3 (Pin A7)	Localización 4 (Pin B0)
Slot 1	INTA	INTB	INTC	INTD
Slot 2	INTB	INTC	INTD	INTA
Slot 3	INTC	INTD	INTA	INTB
Slot 4	INTD	INTA	INTB	INTC
Slot 5 (si existe)	INTD	INTA	INTB	INTC

1st/ 2nd/3rd/4th/ Available IRQ.

Slot 1/2/3/4 IRQ.

La señal INT# es una solicitud de interrupción que es señalada y manipulada por el Bus PCI. Sin embargo, ya que el sistema operativo usualmente tiene la responsabilidad de manipular la E/S, las INT# deben ser convertidas en una IRQ, si el dispositivo requiere un servicio de IRQ. Implicítamente las IRQ 9 y 10 son mapeadas al Bus PCI, pero cualquier IRQ disponible puede ser utilizada.

Esta opción permite determinar que IRQ's convencionales y en que orden se pueden asociar con una de la INT# disponibles. Los valores posibles son **Auto, 9, 10, 11, 12, 14, 15 y NA.** Fije este valor a **Auto** para dejar que sea el BIOS quien distribuya las IRQ que se usarán.

Elementos de Arquitectura y Seguridad Informática

Used Mem Base Addr.

Esta opción usada en conjunto con "Used Mem Length", le permite fijar un espacio de memoria para tarjetas ISA que no son compatibles con PnP. El valor escogido permite especificar la dirección de comienzo del espacio reservado para esta memoria. Los valores posibles son:

N/A
C800
CC00
D000
D400
D800
DC00

Used Mem Length.

Si su tarjeta ISA no es compatible PnP y requiere de un espacio de memoria para funcionar, especifique aquí el tamaño de esta memoria para que el BIOS PnP reserve este espacio para la tarjeta Legacy ISA instalada. Los posibles tamaños de memoria son:

8 K
16 K
32 K
64 K

PCI IRQ Activated By.

Esta opción permite fijar la forma mediante la cual el Bus PCI reconocerá la activación de una señal IRQ proveniente de un dispositivo o controlador. Es recomendable, bajo cualquier circunstancia, dejar esta opción en su valor implícito por que puede afectar grandemente el funcionamiento del sistema. Sólo debe cambiarse si el fabricante del dispositivo o controlador lo recomienda expresamente. Los valores posibles son:

Level (Implícito)	Activación de la IRQ por nivel
Edge	Activación de la IRQ por flanco.

CPU to PCI Write Buffer.

Cuando está activado, permite que los accesos de direcciones y datos sean a un buffer interno del Chipset PCI (82C586), de manera que el procesador pueda ser liberado de estados de espera.

PCI Dynamic Bursting.

Cuando está activado permite que el controlador PCI permita transferencias de ráfagas si los ciclos consecutivos del bus PCI tienen sus direcciones dentro de un espacio de 1 KB. Esta opción permite aumentar la velocidad de transferencia del BUS PCI.

Assign IRQ For VGA.

Si su tarjeta de video no necesita una IRQ, desactive esta opción, por tanto una IRQ puede liberarse para el uso del sistema.

Nota: En ocasiones esta opción esta entre las opciones del Menú CHIPSEP FEATURES SETUP. Pero el resultado es el mismo.

NCR SCSI BIOS.

El valor **Auto**, permite utilizar el NCR SCSI BIOS que está integrado en la ROM BIOS de la Tarjeta Madre y que da soporte a los HDD's SCSI para varios S.O. Es necesario contar con una tarjeta controladora NCR 53C810 en el sistema, para usar este BIOS. Si no tiene este tipo de tarjeta desactive esta opción.

Capítulo IX. Opciones del Menú INTEGRATED PERIPHERALS.

Esta opción permite configurar los dispositivos de Entrada/Salida, integrados sobre la tarjeta madre. En ocasiones los parámetros que se pueden encontrar en este Menú se encuentran ubicados en **CHIPSEP FEATURES SETUP**, y en el menú principal no existe esta opción. No obstante los parámetros son básicamente los mismos. Puede aparecer también con el nombre **I/O CONFIGURATION SETUP**.

IDE HDD Block Mode.

Esta opción permite aumentar la velocidad del Disco Duro ya que habilita la transferencia de datos multisector en vez de la transferencia de un solo sector por interrupción. La mayoría de los discos duros, excepto los muy viejos, soportan esta propiedad.

IDE 32-bit Transfer Mode.

Activando esta opción se permiten transferencias de 32 bits, aumentando los accesos a los datos del disco duro.

PCI Slot IDE 2nd Channel.

Active esta opción si Ud. tiene una tarjeta controladora IDE PCI conectada y la configura como un controlador IDE secundario.

On-Chip Primary IDE / Onboard Primary IDE.

On-Chip Secondary IDE / Onboard Secondary IDE.

Este parámetro permite activar o desactivar los controladores IDE Primario y Secundario sobre la tarjeta madre.

IDE Primary Master PIO.

IDE Primary Slave PIO.

IDE Secondary Master PIO.

IDE Secondary Slave PIO.

Elementos de Arquitectura y Seguridad Informática

Estos parámetros permiten fijar los modos PIO soportados por los discos duros (amo y esclavo) conectados en los canales IDE. **PIO** o **Programmed Input/Output** evita que el BIOS tenga que emitir una serie de comandos para hacer las transferencias hacia o desde el HDD, en vez de esto PIO permite que el BIOS diga al controlador que operaciones quiere realizar y deja que este y el CPU ejecuten ellos mismos la operación. Esto es más simple y eficiente. Existen 5 modos diferentes que difieren enter sí en el atiemppamiento que permiten. Seleccione **Auto** para detectar automáticamente el modo PIO de su disco duro. Los valores posibles son:

IDE Ultra DMA mode.

Permite activar el modo Ultra DMA/33, si es soportado por el disco duro conectado en algún canal IDE. Esta es una nueva especificación para aumentar los rangos de transferencia de datos de los HDD. Al contrario del modo PIO que solo usa el flanco de subida de la señal IDE para transferir los datos, el modo DMA/33 usa los dos flancos, el de subida y de caída. De aquí que se duplican los rangos de transferencias de datos Modo PIO 4 o el Modo DMA 2. (16,6 Mb/s x 2 = 33 MB/s). Seleccione **Auto** para que el BIOS automáticamente ajuste o desactive esta opción para los discos instalados.

La siguiente tabla lista los rangos de transferencias de datos de los Modos PIO y DMA de los discos IDE. El bus IDE tiene 16 bits de ancho, lo cual significa que cada transferencia son dos Bytes.

Modo	Rangos de transferencias
PIO Mode 0	3,3 MB/s.
PIO Mode 1	5,2 MB/s.
PIO Mode 2	8,3 MB/s.
PIO Mode 3	11,1 MB/s.
PIO Mode 4	16,6 MB/s.
DMA modo 0	4,16 MB/s.
DMA modo 1	13,3 MB/s.
DMA modo 2	16,6 MB/s.
Ultra DMA/33	33 MB/s.

Onboard FDC Controller.

Activando esta opción se puede utilizar el controlador de torres de Floppy incorporado en la tarjeta madre. Desactívela si va a usar una tarjeta controladora separada.

Onboard Serial Port 1.

Onboard Serial Port 2.

Estas líneas permiten asignar las direcciones y las IRQ's para los conectores de puerto serie incorporados en la tarjeta madre. Asegúrese de que los puertos series tienen diferentes asignaciones para evitar conflictos.

Valor	Explicación.
3F8 / IRQ4	Puerto serie con la dirección 3F8 usando la IRQ 4. Implícito para COM 1.
2F8 / IRQ3	Puerto serie con la dirección 2F8 usando la IRQ 3. Implícito para COM 2.
3E8 / IRQ4	Puerto serie con la dirección 3E8 usando la IRQ 4.
2E8 / IRQ3	Puerto serie con la dirección 2E8 usando la IRQ 3.
Disable	Desactiva los Puertos Serie.

UART 2 Mode.

Esta opción permite fijar el modo de trabajo del Puerto Serie 2. En las tarjetas en las que aparece esta opción esta disponible un conector para Puerto infrarrojo donde se conecta un modulo IR, el cual se trabaja como si fuera el Puerto Serie 2. Los modos posibles son:

Standard	Prepara al puerto 2 para trabajar en el modo normal. Este es el valor implícito.
HPSIR	Seleccione esta opción si tiene módulo infrarrojo conectado. Este modo permite una comunicación serie infrarroja a una velocidad máxima de 115 K baudio.
AskIR	Seleccione esta opción si tiene módulo infrarrojo conectado. Este modo permite una comunicación serie infrarroja a una velocidad máxima de 19.2 K baudio.

IR Duplex Mode.

Este parámetro permite fijar el modo Duplex para la comunicación infrarroja (IR). Esta función aparece solamente si la función IR está activada y el parámetro **UART 2 Mode** no está puesta en Standard. Los valores posibles son:

Full	Permite la comunicación IR en modo bidireccional.
Half	Permite la comunicación IR en una sola dirección.

Onboard Parallel Port.

Este parámetro controla el funcionamiento del conector de puerto paralelo sobre la tarjeta madre. Si usa una tarjeta multi I/O con un puerto paralelo asegúrese de asignarles diferentes direcciones a cada puerto para evitar conflictos. Las opciones para este parámetro son:

3BC / IRQ7	El puerto paralelo utiliza la dirección de puerto 3BC con la IRQ 7.
378 / IRQ 7	El puerto paralelo utiliza la dirección de puerto 378 con la IRQ 7.

Elementos de Arquitectura y Seguridad Informática

	7.
278 / IRQ 5	El puerto paralelo utiliza la dirección de puerto 278 con la IRQ 5.
Disable	Desactiva el puerto paralelo sobre la tarjeta madre.

Onboard Parallel Port Mode.

Si su sistema tiene un puerto paralelo que soporta los modos extendidos, fije esta opción de acuerdo al modo extendido que soporta su dispositivo paralelo. Los modos posibles son:

Normal	Permite la operación normal en un solo sentido.
Enhanced Parallel Port (EPP).	Permite al puerto paralelo operar en modo bidireccional al máximo de velocidad.
Extended Capabilities Port (ECP).	Permite al puerto paralelo operar en modo bidireccional y a una velocidad mayor que el máximo rango de transferencia.
ECP + EPP	Soporta las facilidades de los modos ECP y EPP

ECP Mode Use DMA.

Esta función permite asignar un canal de DMA para la función ECP del puerto paralelo. Se permite escoger entre los canales de DMA 1 y 3. Siendo el canal 3 el implícito. Este parámetro aparece solamente si en la opción "**Onboard Parallel Port Mode**" se selecciona **ECP** o **ECP + EPP**.

USB Controller.

USB IRQ Released.

Este parámetro permite activar o no los dispositivos USB conectados al sistema si hubiera alguno. El implícito es desactivado.

Nota: La función USB comparte la interrupción INTD# con el Slot PCI 4. Por tanto si activa la función USB, solamente las tarjetas PCI que no requieran interrupción como las tarjetas de video pueden ser instaladas en el Slot 4. El BIOS PnP asigna una IRQ a la VGA solo si esta lo solicita.

USB Legacy Support.

Esta opción permite habilitar o desactivar el manipulador (Driver) del teclado USB que posee el BIOS. Este manipulador simula los comandos de un teclado AT

tradicional y le permite utilizar un teclado USB durante el POST y después de la carga del sistema si **no tiene** un manipulador de USB en el Sistema Operativo. No debe usar al mismo tiempo el manipulador USB del S.O y tener esta opción activada.

Capítulo X. Otras Opciones del Menú Principal.

Load BIOS Defaults.

Esta opción posibilita la carga de los valores permanentes que trae almacenado la ROM BIOS, la carga de dichos valores se encuentra normalmente desactivada, ya que los mismos no son óptimos y deshabilitan las altas prestaciones que puede brindar el sistema. Ejecutar esta opción es útil cuando existen problemas con la tarjeta madre y es necesario identificar la fuente de estos. Cuando se activa este campo aparece en la pantalla de la computadora una confirmación que permitirá actualizar la CMOS con estos valores.

Además, si los valores almacenados en la CMOS RAM se corrompen, el BIOS automáticamente cargará estos valores predeterminados, cuando la máquina despierte.

Estos valores implícitos que se cargan solo afectan las pantallas del **"BIOS Features SETUP"** y **"Chipset Features Setup"**.

Load SETUP Defaults.

Esta opción posibilita la carga de los valores implícitos para el Chipset, los cuales garantizan una optimización máxima de las posibilidades de éste. Estos valores se almacenan en la ROM BIOS del sistema y solo afectan las pantallas del **"Bios Features SETUP"** y **"Chipset Features Setup"**.

Supervisor Password.

User Password.

Estas opciones garantizan la seguridad de la información, ya que limita los niveles de acceso para los usuarios. Permiten fijar, cambiar o desactivar las palabras claves del sistema. La opción **Supervisor Password** permite niveles de acceso, mediante palabra clave, para el sistema y el SETUP al mismo tiempo, mientras que **User Password** solo permite el acceso para el sistema.

Password Setting.

Es otra posibilidad de entrar contraseña para impedir la entrada de intrusos. La contraseña introducida aquí permitirá los niveles de acceso para el SETUP o el sistema, o ambos según sea el valor que tenga la opción **Security Option** en la sección correspondiente al **BIOS FEATURES SETUP**

En cada caso se introduce la contraseña, (hasta ocho caracteres) y el BIOS pide la confirmación de la clave. Para desactivar la opción de seguridad, seleccione alguna de estas en el Menú Principal y de retorno para desactivar la contraseña.

Elementos de Arquitectura y Seguridad Informática

Nota: Si Ud. por alguna razón olvida la contraseña, no podrá entrar al sistema o al SETUP. Para resolver este problema en las tarjetas madres existe un Jumper que permite limpiar la contraseña. Consulte la documentación de su tarjeta madre para determinar la ubicación de este Jumper y el procedimiento a seguir.

IDE HDD Auto Detection.

Al seleccionar esta opción, el programa automáticamente investiga los valores de la geometría correspondiente a todos los discos duros del sistema, brindando diferentes posibilidades de configuración, teniendo en cuenta el modo empleado para definir la geometría del disco (LBA, Large o Normal).

La selección escogida se almacenará en el tipo USER, en la sección **STANDARD CMOS SETUP**, ignorándose de esta forma los valores anteriores del tipo que tenía asignado a sus discos. Si su disco fue formateado con un juego de parámetros diferente a los detectados, Ud. debe entrarlos de forma manual para permitir el acceso a la información que contiene el disco.

HDD Low Level Format.

Esta opción activa un utilitario de formateo de discos duros a bajo nivel, el cual busca automáticamente la información necesaria para el disco seleccionado y ejecuta la operación de formateo. Este utilitario no es recomendable utilizarlo con discos IDE, ya que estos vienen formateados a bajo nivel de fábrica y esta operación pudiera dañarlos del todo. No obstante, existen experiencias de algunos discos que han soportado este procedimiento y se han resuelto los problemas que presentaban, de todas formas solo use esta opción en caso extremo.

SAVE AND EXIT SETUP.

Este campo posibilita que todos los valores actualizados, con los que trabajará su computadora, sean guardados en la CMOS RAM antes de salir y cargar el sistema.

EXIT WITHOUT SAVING.

Seleccione esta opción, Si Ud. desea salir de SETUP sin que los nuevos valores o cambios realizados en él se almacenen en la CMOS RAM.

X. Bibliografía consultada

1. El IBM PC a Fondo. Técnicas y Programación Avanzada.
2. Apuntes para preparación del CD-ROM "Los misterios de la PC". Ing. Guillermo Lastre Olazábal
3. La Rutina POST en la PC. Leopardo Parra Peynada. Centro Japonés de Información Electrónica.
4. El Chipset en la PC. El máximo responsable...Ing. Guillermo Lastre Olazábal.Citmatel. (Presentación Electrónica)
5. Impresoras sin Impacto. Juan José Antonio Maders
6. Misterio de la PC. Los secretos del SETUP del BIOS Award. Ing. Guillermo Lastre Olazábal.Citmatel.
7. Manual de Circuitos Básicos. Ing. Lázaro Leal Moya.
8. Memoria en las PC. . Ing. Guillermo Lastre Olazábal.División Sistemas de Cómputo.CEDISAC. 1998
9. Manual sobre los Buses de las Computadoras. Ing. José Seijas Chávez. CEDISAC
10. <http://www.members.xoom.com/manuales>
11. Manual de Tarjetas Madres. Ing. José Seijas Chávez.
12. <http://www.abcdatos.com/manuales/hardware>
13. [http// www.conozca su hardware.com.](http://www.conozca_su_hardware.com)
14. PC MAGAZINE Edición Española. (número 67, febrero 1994 y número 121).
15. Microsoft Windows Plataforma 2000. Documento oficial sobre Windows 98
16. <http://www.award.com/>
17. <http://www.ami.com/>
18. <http://www.aopen-usa.com/>
19. <http://www.phoenix.com/>
20. "Operación y programación de computadores", de Guinzburg.
21. Revista "Enciclopedia Práctica de la Informática". Octubre de 1984.

Elementos de Arquitectura y de Seguridad Informática

22. Revistas Gigas No.1/1997 y No. 2/1997 en formato digital.
23. Conferencia: Titulo: SETUP DEL BIOS.Autor: Mercedes Sosa Hernández.División de Sistemas de Cómputo. CEDISAC.
24. Memorias Cache. V. Viñals, C. Rodriguez, A. Olivé. Revista Mundo Electrónico, 1986, No 167.
25. PC WORLD España No. 156 Julio 1999. Lectores DVD .Procesadores de 64 Bits.
26. Guía Completa de Mantenimiento y Actualización de la PC, SegundaEdición, por Mark Minasi (1994 por Ventura Ediciones, S.A. de C.V.