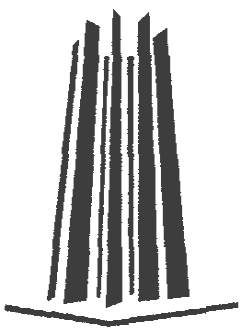
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

INGENIERÍA MECÁNICA ELÉCTRICA

"MANTENIMIENTO DE EQUIPO DE COMPUTO EN LA DIRECCIÓN GENERAL DE TELEVISIÓN EDUCATIVA (DGTVE)"

T E S I S
QUE PARA OBTENER EL TITULO DE
INGENIERO MECÁNICO ELÉCTRICO
P R E S E N T A :
JUAN FERNANDO TORRES CRUZ

ASESOR: ING. JUAN GASTALDI PÉREZ



SAN JUAN DE ARAGON, EDO. DE MÉXICO, MARZO 2006

DEDICATORIA

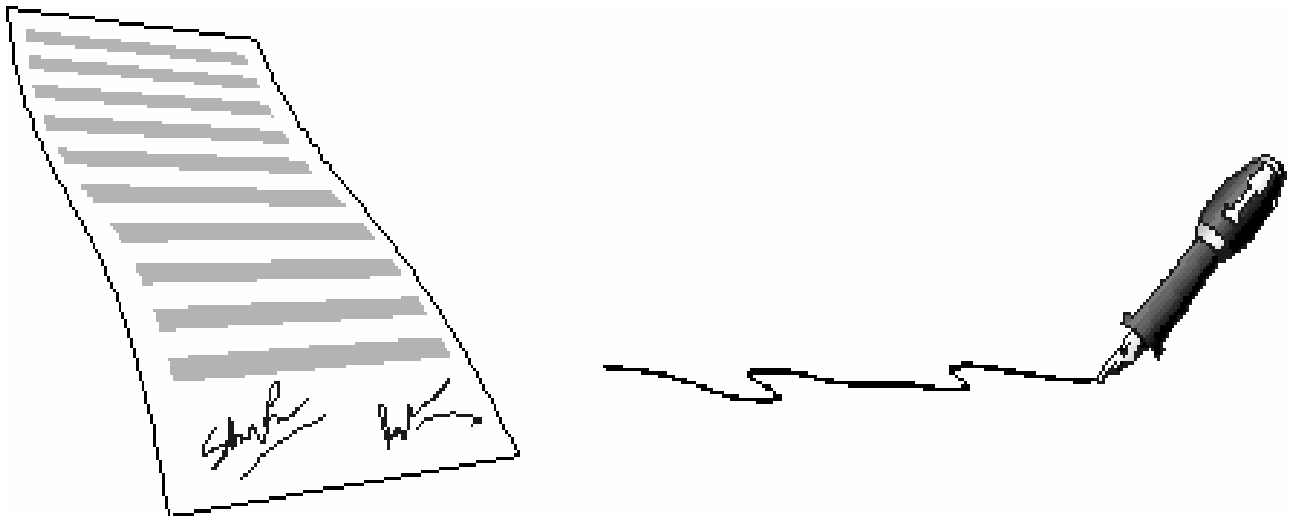
Dedico este trabajo de tesis a mis padres:
Rosa María Cruz Flores y Juan Torres Mancilla,
Por el apoyo y amor que me han dado en estos 25 años
De mi existencia; también se la dedico a mis
Hermanos (Francisco Miguel, Alma Rosa y Juanita),
A mí cuñado (José Guadalupe) y
A mí sobrino (Juan Luís).

AGRADECIMIENTO

Agradezco a la Dirección General De Televisión Educativa
En especial al Laboratorio de Informática de esta institución,
Por ayudarme a la realización de este trabajo, así como por
Hacerme grata la estancia durante mi Servicio Social y Prácticas
Profesionales: a Ángel Cruz, Francisco Lechuga, Juan
Carlos Olvera, Maricela Casarez y Luis Licona.

También les doy las gracias a todos los profesores de la carrera
De Ingeniería Mecánica Eléctrica - Facultad de Estudios Superiores Aragón
De nuestra máxima casa de estudios la Universidad Nacional
Autónoma de México, por haberme dado los conocimientos necesarios
Para enfrentarme a este Mundo cada día más globalizado y loco.

Y por último, agradezco la amistad de todos mis amigos,
Compañeros y conocidos que tuve la dicha de tener durante
Mi etapa de estudiante.



"POR MI RAZA HABLARÁ EL ESPÍRITU"
Bosques de Aragón, Estado de México, Marzo de 2006.

Í N D I C E

CAPITULO 5 MANTENIMIENTO PREVENTIVO Y CORRECTIVO PARA PC's DE LA DGTVE

INTRODUCCIÓN

El presente trabajo de tesis es el resultado de una ardua recopilación de información referente a la Electrónica de las Computadoras y del Sistema Operativo Windows, esto durante mi etapa de estudiante de la carrera de Ingeniería Mecánica Eléctrica y como prestador de servicio social en la Coordinación de Informática de la Dirección General de Televisión Educativa (DGTVE).

Además, con esto pretendo formar un precedente bibliográfico para poder darle Mantenimiento Preventivo y Correctivo a equipos de cómputo en la DGTVE, así futuros prestadores de la FES Aragón especialmente de la carrera de Ingeniería Mecánica Eléctrica pueden tener a su alcance y disponibilidad una fuente de consulta que los oriente, puesto que es muy poco lo que se nos da respecto a este tema en la Licenciatura, pero esto no quiere decir que no les sirva a otros profesionista de otras licenciaturas de la FES o incluso de otras instituciones públicas o privadas; cualquiera podrá acceder a dicha información y así poder realizar un buen trabajo en estos equipos, no importando de que marca sean o que tan robustos se vean.

Para lo cual divido este trabajo en los siguientes capítulos:

En el capitulo 1 doy una breve introducción de lo que es la Dirección General de Televisión Educativa, su misión, visión y propósito en la fomentación y difusión de la educación en México, su estructura y una breve reseña histórica de sus orígenes.

En el capítulo 2 menciono la descripción de la Arquitectura de una Computadora, así como una breve reseña histórica y algunos conceptos básicos para ayudar a todos aquellos que tengan duda sobre algunos tecnicismos del área de informática, así como la estructura básica de un sistema informático y sus partes, principalmente el Hardware (dispositivos de entrada y salida).

En el capítulo 3 me adentro al tema del Software esa parte lógica e intangible y que ha facilitado el uso de la computadora, su estructura, tipos de software y hago una breve explicación de la memoria BIOS uso, configuración y errores que se llegan a presentar durante el arranque de la misma.

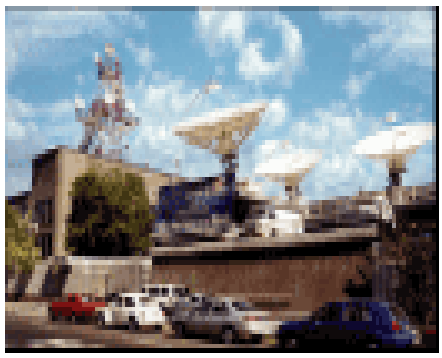
En el capítulo 4 que para mi opinión es uno de los más extensos pero muy importante e interesante, ya que hablo de las amenazas que hoy en día padecen todos equipos informáticos y que todos hemos oído hablar de ellos “los virus informáticos”, pero si no fuera bastante con ellos, se suman a estos nuevos programas maliciosos englobados en un solo termino malwares (spyware, spam, gusanos informáticos y troyanos) y que hacen que uno tenga dolores de cabeza cuando se introducen en nuestro ordenador provocando destrozos en nuestro sistema e información que tengamos almacenada en ella.

Por ultimo, en el capítulo 5 hablo de las medidas preventivas y correctivas que le damos a los equipos de cómputo en la DGTVE e incluso pueden aplicarse a cualquier equipo que sea o no sea de la institución, estas medidas son al Hardware (todo el equipo físico) y al Software (sistema operativo y demás programas que estén instalados) para hacer que funcione adecuadamente.

En la parte final de este trabajo doy mis conclusiones y presento una lista de las fuentes de información consultadas de las cuales me base para hacer esta tesis, además les puede servir a todos aquellos que quieran profundizar en algún tema en específico y así poder aclarar sus dudas.

CAPITULO 1
LA DIRECCIÓN GENERAL DE TELEVISIÓN EDUCATIVA

1.1Introducción

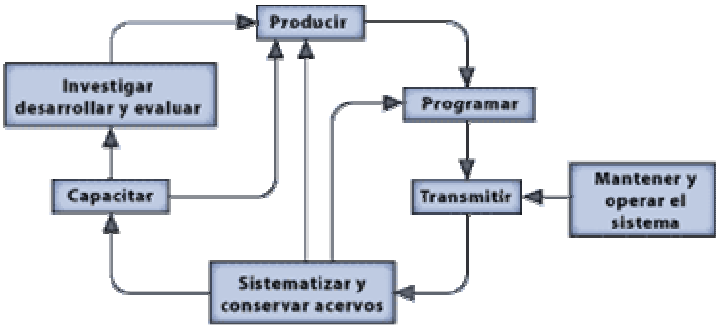


La Dirección General de Televisión Educativa (DGTVE) es un órgano centralizado de la Secretaría de Educación Pública, dependiente de la Unidad de Planeación y Evaluación de Políticas Educativas.

Las tareas a cargo del personal que integra la DGTVE son producir, programar y transmitir contenidos educativos a través de medios electrónicos, principalmente la televisión, mediante la Red EDUSAT.

Sin embargo, el trabajo no concluye con la transmisión, ya que también son esenciales las labores de mantenimiento y operación técnica de la Red EDUSAT, la sistematización y la conservación de los acervos audiovisuales, la formación y la capacitación de profesionales en materia de audiovisual educativo, y la realización de actividades de investigación, desarrollo y evaluación.

Todas estas tareas integran un ciclo que ha permitido, a lo largo de más de 35 años de actividad, explorar y descubrir las importantes potencialidades del audiovisual educativo como una herramienta de gran alcance que sin duda ha facilitado llevar educación y conocimientos a las zonas más remotas y desprotegidas del país, a un amplio abanico de usuarios, a través de diversas modalidades, niveles y contenidos educativos.



1.2 Propósito

Ofrecer condiciones que permitan el ejercicio pleno del derecho a la educación de cada individuo mediante el uso de tecnologías de información y la comunicación (TICs), proporcionando servicios educativos en los lugares más apartados y de difícil acceso del país, con la finalidad de beneficiar a las regiones con mayor rezago educativo, así como a la sociedad en general. Esas condiciones estarán basadas en los principios de justicia y de equidad educativas y se concretarán con la consolidación, la ampliación y la actualización de la infraestructura tecnológica y el diseño de modelos de enseñanza apoyados en las TICs

conjuntamente con la producción, la distribución y la sistematización de material audiovisual e informático como apoyo a la educación.

1.3 Misión

La misión de la Dirección General de Televisión Educativa (DGTVE) es brindar condiciones para que todas las personas en México puedan ejercer su derecho a la educación. Lograr un esquema de equidad en materia educativa resulta complicado, especialmente en zonas apartadas y de difícil acceso, por lo que nuestra labor, como difusores del conocimiento a través de medios electrónicos, se enfoca de manera puntual hacia aquellas regiones con mayor rezago educativo.

1.4 Visión

La visión de la DGTVE para el año 2025 contempla aprovechar al máximo las tecnologías de información y comunicación (TICs) para llevar la educación con calidad y con equidad a los rincones más apartados del país y con mayor rezago educativo. Para ello, se plantea actualizar el equipo y la infraestructura existentes, ampliar y diversificar la cobertura de la señal, desarrollar nuevos modelos pedagógicos apropiados para el uso de las TICs en la educación, capacitar a especialistas en el uso del audiovisual, así como contar con material de apoyo para ofrecer a toda la población oportunidades de desarrollo basadas en el respeto a la legalidad y el ejercicio real de los derechos humanos.

1.5 Objetivo - Tareas

El Programa Nacional de Educación 2001-2006 establece tres grandes desafíos que debe afrontar la educación nacional:

1. Cobertura con equidad (educación para todos).
2. Calidad de los procesos educativos y niveles de aprendizaje.
3. Integración y funcionamiento del sistema educativo (educación de vanguardia).

Considerando estos desafíos, en paralelo con la emergencia y el avance de las tecnologías de información y comunicación (TICs) y su impacto en la vida social, la DGTVE redimensiona y redirecciona sus estrategias, sin perder de vista su objetivo fundacional, que es contribuir al abatimiento del rezago educativo en México.

Así, a la par que se mantiene y amplía en forma cualitativa y cuantitativa la cobertura de los servicios educativos utilizando como herramienta fundamental la televisión vía satélite a través de la Red Edusat, la DGTVE desarrolla funciones dentro del Programa de Expansión del Uso de las Tecnologías de Información y Comunicación en la Educación Básica, dentro del cual le han sido asignados dos subprogramas bajo su responsabilidad:

- Mejoramiento de la Operación y Expansión de la Red Edusat
- Operación y Consolidación de la Videoteca Nacional Educativa

Como resultado del esfuerzo sostenido de la DGTVE por mejorar y ampliar sus servicios, actualmente la Red Satelital de Televisión Educativa (Edusat), sistema de señal digital comprimida, es el más importante de su naturaleza en Latinoamérica. Transmite diariamente 14 canales de televisión, diez de ellos con programación propia (canales 11, 12, 13, 14, 15, 16, 17, 18, 27 y Aprende TV) y cuatro con retransmisión de señal mediante

convenios (canales 22, 23, 25 y 26), así como cuatro de radio (canales 15, 25, 26 y 28), a un total de 30 mil puntos receptores en México y en casi todo el Continente Americano.

La Dirección General de Televisión Educativa (DGTVE) administra los canales 11, 12, 14, 17, 27 y Aprende TV y el Instituto Latinoamericano de la Comunicación Educativa (ILCE) tiene a su cargo los canales 13, 15, 16 y 18. Los canales con retransmisión son: el 22, con la programación del Canal 22 Internacional, el Canal 23, a cargo del Centro Nacional de las Artes (CENART), el 25 al cual corresponde la señal del Canal del Congreso y el 26, Canal de la Presidencia de la República.

Las tareas sustantivas a través de las cuales la DGTVE cumple con su objetivo son:

• **Operación de la Red Edusa**t, que abarca los ámbitos de programación y transmisión de programas educativos, para televisión y radio, así como la operación y el mantenimiento preventivo y correctivo de la Red Edusat.

• **Producción audiovisual**, entendida como la concepción y la realización de series y programas educativos, acordes a las necesidades de diferentes públicos.
• Servicio Nacional de Imagen Educativa, que comprende conservación y sistematización de acervos.

• **Formación, capacitación y actualización** para profesionales vinculados con los medios audiovisuales educativos.

• **Investigación**, desarrollo audiovisual y evaluación.

• **Intercambio de experiencias**, información y materiales con instituciones y organismos que participan en la educación a través de los medios audiovisuales, así como con sistemas de televisión en diversos puntos del país.

1.6 Estructura

La DGTVE está conformada por una Dirección General que agrupa a las siguientes áreas:

• **Dirección de Producción.** Tiene a su cargo la concepción y la realización de series y programas de televisión educativa, en función de las necesidades de los variados públicos a los que se dirigen las transmisiones, para diferentes niveles y modalidades de enseñanza, en congruencia con los propósitos del Sistema Educativo Nacional.

• **Dirección de Vinculación Institucional y Desarrollo Audiovisual.** Promueve la difusión de los servicios de producción, transmisión y resguardo del acervo audiovisual de la DGTVE, a través de medios electrónicos e impresos. También establece líneas de colaboración en la difusión y la producción de programas educativos de televisión con instituciones y organismos públicos y privados.

Asimismo, tiene a su cargo las investigaciones en torno a la producción, al uso y a la recepción de los programas educativos. Es también responsabilidad de esta área la programación y la continuidad de los canales de la Red Edusat.

• **Dirección de Ingeniería.** Tienen la responsabilidad de todas las actividades técnicas de instalación, manejo y mantenimiento del equipo para la producción y la transmisión de los programas educativos de la DGTVE. Brinda además, asesoría técnica, orientación y capacitación a usuarios de la Red Edusat.

• **Centro de Entrenamiento de Televisión Educativa (CETE).** Instrumenta servicios educativos relacionados con la formación y la capacitación profesional en comunicación audiovisual, a través de cursos presenciales y a distancia, en los ámbitos de la producción y del uso del audiovisual educativos, dentro y fuera del aula. Todos los programas de formación, capacitación y actualización que brinda el CETE, cuentan con reconocida calidad internacional e incluyen la debida acreditación para los participantes que los concluyen satisfactoriamente. Asimismo, los programas contemplan el uso de material didáctico de apoyo.

• **Videoteca.** Se concibe como una estrategia interinstitucional entre la Dirección General de Televisión Educativa (DGTVE), la Dirección General de Tecnología de la Información (DGTEC) y el Instituto Latinoamericano de la Comunicación Educativa (ILCE), a fin de conformar un centro nacional de imagen, para la conservación y el aprovechamiento del acervo audiovisual educativo del país. Para tal efecto se han desarrollado dispositivos de redes informáticas, patrones de sistematización, conservación y referenciación de materiales y contenidos audiovisuales, mismos que han sido concentrados en una plataforma tecnológica de gran alcance.

• **Dirección de Planeación.** Establece las líneas de acción para planear, organizar y operar las actividades y los proyectos asignados a la DGTVE. Asimismo, supervisa que los planes de la dirección se integren a los planes y programas nacionales y sectoriales. Coordina y asesora la elaboración del Presupuesto Anual y la gestión de su aprobación ante las autoridades competentes. También lleva a cabo la evaluación periódica del avance de los proyectos, en lo que toca al cumplimiento de metas y ejercicio de los recursos.

• **Coordinación de Informática.** Entre sus funciones más importantes se cuentan la evaluación y determinación de requerimientos de equipo de cómputo, el diseño y desarrollo de una red de información interna, asesoría a usuarios para el manejo de sistemas, conservación y revisión periódica de los equipos de cómputo a su cargo, así como la supervisión de los servicios de mantenimiento preventivo y correctivo a los mismos, diagnóstico de necesidades de equipo, propuestas y participación en la impartición de cursos de capacitación al personal, de acuerdo con las necesidades detectadas en esta área.

La Dirección General de la DGTVE coordina y supervisa las acciones de todas las áreas que la conforman, a fin de cumplir la misión institucional, mediante la producción, la programación y la transmisión de programas educativos de calidad, con apego a los planes y programas nacionales y sectoriales. Asimismo, conduce la evaluación de las tareas mencionadas. Otra labor importante es la celebración de acuerdos y convenios con organismos afines, de los sectores público, social y privado, nacionales e internacionales. Adicionalmente, emite políticas internas y conduce la administración de los recursos asignados a la DGTVE.

1.7 Breve historia

He aquí los hechos más relevantes que conforman el origen y desarrollo de lo que hoy es la Dirección General de Televisión Educativa (DGTVE).

1964	**Dirección General de Educación Audiovisual** La Secretaría de Educación Pública (SEP) crea la Dirección General de Educación Audiovisual buscando, a través del uso de medios de comunicación, nuevas alternativas de educación con el fin de abatir el rezago educativo, principalmente en zonas rurales. Es importante destacar que el uso de la televisión en el proceso de enseñanza aprendizaje fue iniciativa y responsabilidad del bachiller Álvaro Gálvez y Fuentes.
5 de septiembre de 1966	**Fase experimental de Telesecundaria** Este proyecto comienza como un sistema experimental en circuito cerrado, con la finalidad de desarrollar y evaluar un nuevo modelo pedagógico. Posteriormente es ajustado y aceptado, para convertirse en una nueva modalidad educativa, complementaria a los sistemas tradicionales.
2 de enero de 1968	**Telesecundaria en el Sistema Educativo Nacional** La Telesecundaria queda inscrita al Sistema Educativo Nacional, lo que confiere validez oficial a los estudios realizados a través de esta modalidad.
Años setenta	**Expansión de Telesecundaria** Se expande la cobertura de la Telesecundaria hasta cubrir la totalidad del territorio nacional.
1978	**Dirección General de Materiales Didácticos y Culturales** La Secretaría de Educación Pública (SEP) dispone cambiar la denominación de la dependencia a Dirección General de Materiales y Métodos Didácticos, la cual tiene a su cargo la elaboración de los guiones, la producción y la transmisión de programas de televisión educativos.
1981	**Unidad de Televisión Educativa y Cultural (UTEC)** Un nuevo cambio de denominación se hace necesario, con la ampliación de funciones de la dirección, que ahora también produce series culturales; se convierte entonces en la Unidad de Televisión Educativa y Cultural (UTEC).
1983	**Custodia del acervo audiovisual** Se asigna a la UTEC la custodia de todo el material audiovisual del sector

	educativo y cultural.
1988	**Unidad de Televisión Educativa (UTE)** La entonces UTEC transfiere la programación cultural al recién creado Consejo Nacional para la Cultura y las Artes (CONACULTA), para abocarse exclusivamente a la producción y la transmisión de programas educativos. Cambia su denominación a Unidad de Televisión Educativa (UTE).
12 de diciembre de 1989	**Primera reestructuración** Se gestiona ante la Secretaría de Hacienda y Crédito Público (SHCP) la definición de una estructura orgánica y funciones específicas para esta institución. La nueva estructura reduce a la UTE a una dirección de área, tres subdirecciones y once jefaturas de departamento, y así permanece hasta 1997, año en el que realizan nuevas gestiones.
18 de marzo de 1991	**Convenio México-Japón / Nace el CETE** El Centro de Entrenamiento de Televisión Educativa (CETE) es creado con el auspicio de la Agencia de Cooperación Internacional de Japón (JICA), con base en el Acuerdo de Cooperación Técnica firmado el 2 de diciembre de 1986 por los gobiernos de Japón y México.
13 de diciembre de 1995	**Transmisión vía satélite** La UTE inicia la transmisión de programas educativos a través de la Red Satelital de Televisión Educativa (Red Edusat). Se distribuyen antenas parabólicas, decodificadores y televisores a planteles educativos estratégicamente ubicados en todo el país.
1996	**Inicia EMSAD** Inicia el proyecto de Educación Media Superior a Distancia (EMSAD), como una modalidad educativa flexible que permite iniciar, continuar o concluir los estudios de bachillerato a personas sin acceso a la formación escolarizada de este nivel. Los materiales impresos y las transmisiones televisivas son fundamentales en este modelo.
1996	**Proyecto de la Videoteca Nacional Educativa** Se inicia la gestión para el desarrollo del proyecto de la Videoteca Nacional Educativa (VNE), a partir del convenio de colaboración establecido entre la SEP y el Instituto Latinoamericano de Comunicación Educativa (ILCE), en materia de educación a distancia.
31 de marzo de 1997	**Inicia el proceso de la segunda reestructuración de la UTE** Se presenta ante la SHCP la propuesta de modificación estructural de la UTE, con el fin de ampliar su capacidad de operación.

31 de marzo de 1999	**Dirección General de Televisión Educativa (DGTVE)** La SHCP determina procedente la modificación de estructura de la UTE. La nueva denominación del organismo es Dirección General de Televisión Educativa (DGTVE).
2000	**Puesta en marcha de la Videoteca Nacional Educativa** Se pone en marcha el proyecto de la Videoteca Nacional Educativa, cuyo objetivo es el desarrollo de procesos de conservación, preservación y documentación de material y contenido audiovisual, mediante el uso de una plataforma tecnológica de gran potencia.
Actualmente	La operación y la programación de los 12 canales que transmite la Red Edusat requiere la concurrencia de los esfuerzos de dos instancias: la DGTVE y el ILCE, Instituto Latinoamericano de la Comunicación Educativa. Al día de hoy, la DGTVE y el ILCE emiten la señal de Edusat a 30 mil equipos receptores en todo el territorio nacional, y alcanzan a un amplio público en Canadá, Estados Unidos, Centro y Sudamérica. Además, se cuenta con señal abierta y por cable en diversos puntos del país.

CAPÍTULO 2
ARQUITECTURA DE UNA COMPUTADORA

2.1 Introducción

Desde que el hombre tuvo la necesidad de contar, se ha enfrentado a tareas rutinarias y repetitivas de cálculo y de gestión. Como respuesta a esta necesidad, el hombre desarrolló herramientas para facilitar la realización de este tipo de trabajos. Estas herramientas fueron evolucionando a lo largo del tiempo hasta llegar a las sofisticadas máquinas de tratamiento de información que hoy en día todos conocemos, las ***computadoras u ordenadores***. Estas máquinas han traído consigo una nueva y optimista ciencia, la informática, que estudia cómo sacarle el mejor provecho a las computadoras para ayudar al hombre en la realización de una gran variedad de tareas. Este nuevo término de informática no debe ser considerado únicamente como ciencia, sino también como tecnología (ciencia y tecnología de las computadoras).

La palabra ***informática*** abarca toda actividad relacionada de cualquier forma con los ordenadores. Desde su aparición, su crecimiento ha sido enorme y ha llegado a involucrar a millones de personas directa o indirectamente. Esta prosperidad de la tecnología informática se debe fundamentalmente a la asombrosa capacidad de realización de tareas que poseen los ordenadores. Hoy en día, los ordenadores influyen en casi todos los aspectos de nuestras vidas y han provocado profundos cambios en múltiples actividades de nuestra sociedad.

2.2 Conceptos Básicos

Informática.- El origen de este término obedece a la fusión de los términos INFORmación y autoMÁTICA, y hace referencia al conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático y racional de la información por medio de ordenadores. Aquí se considera como *información* a todo conjunto de hechos y representaciones acerca de algún conocimiento humano en cualquier dominio. En los países anglosajones, se hace referencia a la informática como la ciencia de las computadoras (*Computer Science)*, aunque también está cobrando gran importancia el término *informatics.*

Dato.- Conjunto de símbolos que representa una información de una forma aceptable para ser procesada de alguna forma. Un dato puede ser el peso de una persona (25Kg), su CURP (TOCJ810307HMCRRN04), la superficie de una finca (450 m^2), etc. Los datos, por sí solos, no poseen utilidad, para ello necesitan de una interpretación (dada por los humanos) que les dé sentido.

Ordenador *(Computadora)*: Máquina compuesta de elementos físicos (en su mayoría de origen electrónico) capaz de aceptar unos datos de entrada, realizar con ellos operaciones lógicas y aritméticas con gran velocidad y precisión, proporcionando los resultados a través de algún medio de salida, todo ello es llevado a cabo sin la intervención de un operador humano y bajo el control de un programa de instrucciones previamente almacenados en la propia computadora. Por consiguiente, un ordenador puede ser

considerado como un sistema que acepta unas entradas (datos e instrucciones) y devuelve unas salidas (datos de salida o resultados).

Programa.- Conjunto de órdenes o instrucciones que se le dan a una computadora para realizar un proceso determinado. Las órdenes que integran un programa indican a la computadora las tareas que han de ser realizadas para llevar a cabo el proceso requerido.

Aplicación informática.- Conjunto de programas, junto con la documentación asociada a los mismos, que permiten la completa realización de un determinado tipo de trabajo (tratamiento de textos, facturación, contabilidad, gestión de nóminas, etc.).

Sistema informático.- Conjunto de elementos necesarios para la realización y explotación de aplicaciones informáticas.

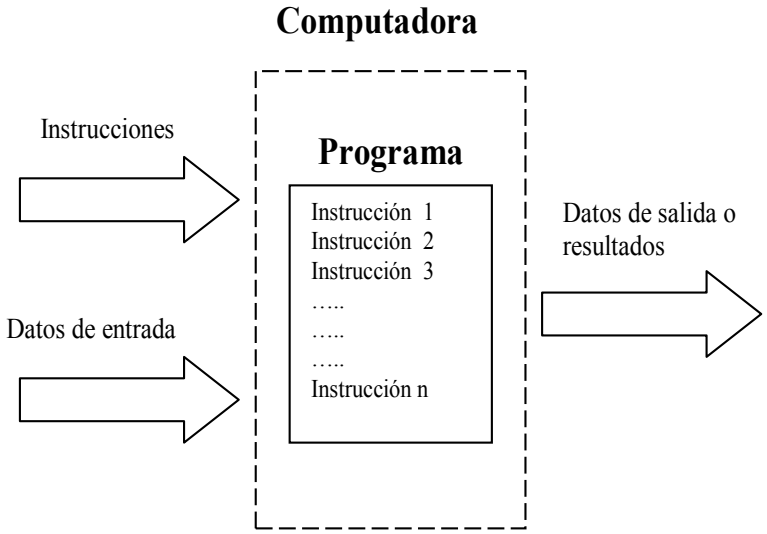


Figura 2.1 Visión abstracta de una computadora

2.3 Representación de la información en un ordenador

Dentro de un ordenador, la información se representa en forma codificada. Una ***codificación*** no es más que una transformación que representa los elementos de un conjunto mediante los de otro, de forma que a cada elemento del primer conjunto le corresponde uno distinto del segundo. Así, por ejemplo, el ADN de una persona es código numérico que se le asigna a cada persona, la fecha no es más que un código utilizado para designar determinadas porciones de tiempo (los días), etc.

En el interior de un ordenador, toda la información es representada según un código que utiliza sólo dos valores (código binario). Estos valores hacen referencia a dos estados físicos determinados que son posibles en una máquina de origen electrónico y que son representados generalmente como **0** (apagado, no pasa corriente eléctrica o luz) y **1** (encendido, pasa corriente eléctrica o luz). Naturalmente, la información que proviene del exterior debe ser transformada a este código para poder ser procesadas por la computadora, y la información resultante del procesamiento debe ser transformado a otros códigos que puedan ser entendidos por los usuarios o cualquier otro elemento externo. Estas transformaciones entre códigos son realizadas de forma automática.

Para cuantificar la información se utilizan determinadas unidades. La unidad mínima de información es el **bit** (**bi**nary digi**t**). Un bit representa la cantidad de información que aportaría el conocimiento del resultado de un proceso que puede dar lugar a dos posibles resultados. Por ejemplo, el conocimiento del resultado obtenido al lanzar una moneda (los posibles resultados son cara y cruz) aporta un bit de información.

No obstante, dado que el bit es una unidad de información demasiado elemental, se utiliza una unidad mayor para representar la capacidad de almacenamiento de un ordenador, el byte. Un **byte** es el número de bits necesarios para almacenar un carácter (generalmente son 8 bits, por lo que se habla también de octeto). Al igual que ocurre con otras unidades, es muy usual utilizar múltiplos del byte:

- **1 Kilobyte** (1KB) = 2^{10} bytes = 1024 bytes
- **1 Megabyte** (1MB) = 2^{20} bytes = 1024 KB
- **1 Gigabyte** (1GB) = 2^{30} bytes = 1024 MB
- **1 Terabyte** (1TB) = 2^{40} bytes = 1024 GB
- **1 Petabyte** (1PB) = 2^{50} bytes = 1024 TB

2.4 Breve Cronología Histórica

Un breve repaso por cinco milenios permite obtener una visión clara de cómo en poco más de treinta años el devenir de los acontecimientos nos ha hecho ser protagonistas de uno de los mayores avances tecnológicos de la Historia.

3000 a.C.	Se encuentra la referencia al primer ábaco (el mismo ingenio que se repite históricamente hace 2500 años en China y 100 años a.C. en Roma).
2000 a.C.	Se escribe el *libro de las mutaciones* o *I-Ching* en China. Se trata de una aproximación al sistema binario, base de los sistemas digitales utilizados en la actualidad.
600 a.C.	En el libro XVIII de *La iliada de Homero*, hay una referencia literaria a un autómata.
500 a.C.	Tales de Mileto define la electricidad estática, obteniendo de su texto la palabra “electrón”.
100 a.C.	Herón de Alejandría construye el primer robot, con fines lúdicos basado en sistemas hidráulicos.
1642	Blaise Pascal, con tan sólo 19 años crea la primera máquina capaz de sumar.
1666	Samuel Morland construye la primera máquina capaz de realizar operaciones que, hasta el momento, sólo se atribuían a los humanos sobre la base previamente establecida por el francés Blaise Pascal.
1671	Se implementa la máquina multiplicadora de la mano de Gottfried W. Leibniz, matemático alemán, llegando a multiplicar y dividir.
1800	Dorr E. Felt inventará una calculadora a la que se denominará *Comptómetro.*
1800	Bill S. Burroughs diseña una sumadora capaz de *recordar* el resultado de la operación anterior (inicios del concepto de memoria).
1821	Charles Babbage, profesor en la Universidad de Cambridge que en 1821

presenta ante la Royal Astronomical Society su “máquina de diferencias”, capaz de resolver ecuaciones polinómicas mediante el cálculo de las diferencias sucesivas entre los conjuntos de números.

1822 La máquina de Charles Babbage es premiada en 1822 con la Medalla de Oro de la Royal Astronomical Society.

1847 George Boole publica *El análisis matemático del pensamiento* dando las bases de “su álgebra”: el Álgebra de Boole.

1878 Ramón Verea desarrolla una máquina capaz de dividir y multiplicar directamente sin el uso de tablas. Verea se negó a la comercialización de la máquina argumentando que su único motivo para el diseño era demostrar la capacidad creadora española (paradójicamente este señor residía en Nueva York).

1890 Bajo el respaldo comercial de “Tabulating Machine Company”, aparece la máquina tabuladota de Herman Hollerith, basada en los ensayos de Boole y Babbage.

1903 Nace John Von Neumann, matemático de origen húngaro nacido en Budapest.

1912 Nace el ilustre matemático británico Alan Mathison Turing. Con una vida tortuosa, aporta numerosos avances en Inteligencia Artificial así como en sistemas de codificación de información.

1913 A. Meisner diseña la primera válvula de vacío, elemento electrónico previo al transistor.

1914 Leonardo Torres y Quevedo escribe *Ensayos sobre la Automática* donde define una máquina que opera según unas reglas previas definidas (metodología de la programación).

1924 T. J. Wason, comercial de CTR ve claras posibilidades de negocio en las máquinas interpretadoras de tarjetas perforadas y crea su propia compañía: la *Internacional Business Machina*, más popularmente conocida como IBM.

1932 James Bryce (IBM) trabaja en un proyecto de implementación de válvulas de vacío en máquinas calculadoras.

1934 El alemán Honrad Zuse desarrolla dos máquinas denominadas Z1 y Z2 bastante similares a un ordenador actual entre 1934 y 1939.

1937 Se firmó un convenio entre IBM y la Universidad de Harvard para el desarrollo de una máquina electromecánica basada en relés.

1941 J. W. Manchyl desarrolla un proyecto que servirá de base años después para desarrollo del ENIAC.

1943 Se destruye el Z3 en un bombardeo. Una réplica de la máquina se encuentra en el Museo Deutsche de Munich.

1943 Alan Mathison Tuning y Tommy Flowers construyen “Colossus”, una máquina encargada de descifrar los mensajes alemanes codificados en la Segunda Guerra Mundial (lo que hoy se llamaría un ordenador “dedicado”), formado por 2400 válvulas, 5 paneles de entrada de datos con tarjetas perforadas y un rudimentario sistema de impresión.

1944 El convenio IBM-Harvard firmado en 1937 para el desarrollo de una máquina electromecánica basada en relés, da sus frutos: el MARKI.

1945 Turing trabaja en el Laboratorio Nacional de Física intentando construir una máquina a semejanza del cerebro humano, que no llegó a buen puerto al desconocer otras disciplinas como la neurofisiología.

1947 John Bardeen, Walter Brattain y William Shockley, ingenieros de los

Laboratorios Bell, consiguen sustituir a las válvulas de vacío con un nuevo elemento basado en semiconductores: el transistor.

1949 John Von Neumann aporta una solución a la programación del ENIAC: ya no será preciso recablear físicamente la máquina, sino que las operaciones a realizar también se introducirán en la máquina a través de tarjetas perforadas.

1951 La Oficina del Censo de los EE.UU. adquiere una máquina UNIVAC I para procesar el censo del año anterior.

1953 Comienza la fabricación de los IBM 701 de las que entre 1953 y 1957 se fabricarán 18 unidades.

1955 La utilización de transistores en los ordenadores es por fin real, disminuyendo de forma espectacular en tamaño, consumo, precio y disipación de energía.

1955 Comienza la segunda generación de ordenadores.

1957 Fallece John Von Neumann.

1964 Se inicia la tercera generación de ordenadores.

1964 Aparece el IBM 360

1971 Aparece el primer microprocesador de la historia: el 4004 de Intel.

1974 Se inicia la cuarta generación de ordenadores.

1975 Steve Wozniak y Steve Jobs diseñan su primer ordenador al que llamaron Apple.

1976 Aparece la segunda versión del Apple: el Apple II.

1981 Se venden 800,000 ordenadores a escala mundial.

1981 Aparece el IBM PC XT.

1982 Se vendieron 1,400,000 ordenadores a nivel mundial. Entre 1984 y 1987 las ventas mundiales de ordenadores alcanzaron los 60 millones de máquinas.

1982 Nace la compañía Compaq Deskpro Corporation que se consolidará como uno de los grandes fabricantes de hardware y que posteriormente será absorbida por HP.

1983 Se establece el inicio de la quinta generación de ordenadores, en la que se supone que nos encontramos aún.

1984 Aparece el Macintosh de Apple, como fruto de la experiencia adquirida por máquinas anteriores y, se dice, influenciados por la tecnología de Seros en Palo Alto.

1986 Compaq desbanca como fabricante mundial de PCs a IBM que, hasta el momento había contado con el liderazgo de ventas.

2001 Aparece la “Nueva HP” como fruto de la absorción por parte de Hewlett Packard de la compañía Compaq.

2003 Los microprocesadores funcionan a más de 3 GHZ y esto parece no tener fin. Los límites de velocidad empiezan a vislumbrase como un problema físico.

2.5 Elementos constituyentes de un sistema informático

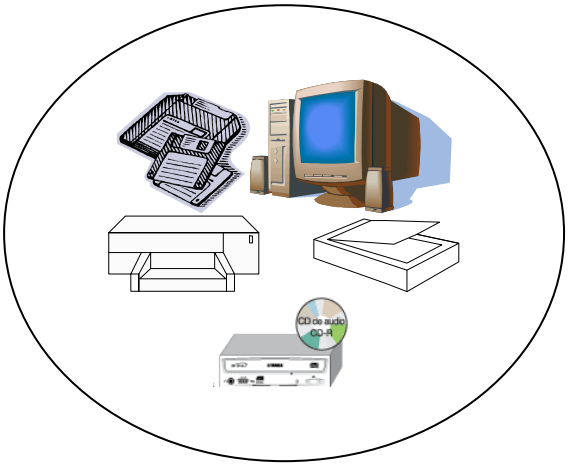


Figura 2.2 Elementos Hardware de un sistema informático

Los cuatro elementos que conforman un sistema informático y que, por consiguiente, hacen posible el desarrollo y aprovechamiento de aplicaciones informáticas son: una parte de naturaleza física (*El Hardware)*, una parte de naturaleza lógica e inmaterial (*El Software)*, una parte humana (integrada por el *personal informático)* y un elemento mixto (*El Firmware)*.

- **Hardware:** Conjunto de materiales físicos que componen el sistema informático, es decir, la propia computadora, los dispositivos externos a la misma, así como todo material físico relacionado con ellos (conexiones, cables, etc.).
- **Software:** Parte lógica del sistema informático que dota al equipo físico de la capacidad para realizar cualquier tipo de tareas. De acuerdo a esta definición, el software integraría al conjunto de programas ejecutables sobre el hardware junto con los documentos y datos asociados a los mismos.
- **Personal informático:** Conjunto de personas que desempeñan las distintas funciones relacionadas con la utilización y explotación de las computadoras en una determinada empresa u organización.
- **Firmware:** Conjunto de instrucciones que las computadoras llevan pregrabadas de fábrica en su propia circuitería (se trata de un concepto intermedio entre software y hardware).

2.6 Esquema Básico del Hardware

El Hardware de un sistema informático está compuesto por todos los elementos del mismo con entidad física, es decir, los cables, los circuitos, los dispositivos electromecánicos, etc. Aquí presentamos una clasificación, desde un punto de vista funcional, de los componentes de un ordenador. Identificaremos y analizaremos cada componente que realice una función bien delimitada dentro de la estructura de la computadora. Por este motivo, en lugar de referirnos a componentes físicos, hablaremos de las unidades funcionales de un ordenador. Un esquema de la estructura de un ordenador típico, de acuerdo a nuestro enfoque funcional, es presentado en la siguiente figura 2.3.

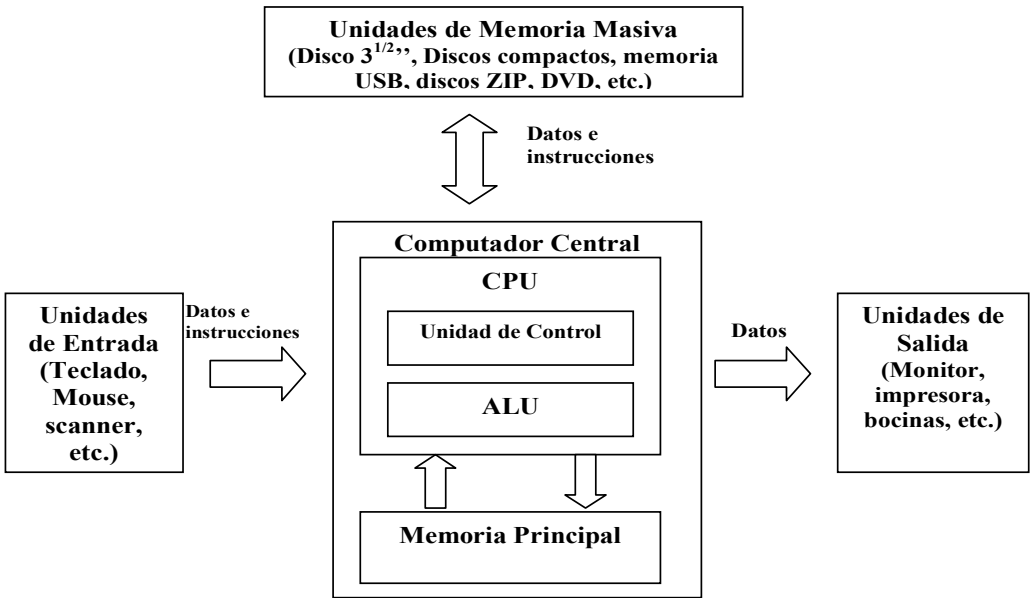


Figura 2.3 Estructura funcional de un ordenador típico

2.7 La Computadora Central

Es el elemento más importante de la computadora, ya que maneja todo el procesamiento, coordinando y realizando todas las operaciones del sistema informático. Podemos distinguir, a su vez, dos unidades funcionales dentro de la computadora central: *la unidad de memoria principal y la unidad central de procesamiento* (CPU):

- **Memoria principal, central o interna:** Es el elemento encargado de almacenar los programas y los datos necesarios para que el sistema informático lleve a cabo algunas tareas. Para que un programa puede ser ejecutado en una computadora, al menos parte del mismo debe encontrarse en memoria principal, junto con los datos que deban ser procesados. Estas memorias presentan gran rapidez y se componen de celdas direccionadas, de forma que cada operación de lectura o escritura en memoria exige la especificación de la dirección sobre la cual se va a realizar dicha operación. Existen dos tipos de memoria principal: la memoria RAM, que permite realizar tanto operaciones de lectura como de escritura y es volátil (si se desconecta el ordenador, se pierde toda la información almacenada), y la memoria ROM, que sólo permite lecturas y es permanente (no necesita ser alimentada con corriente para mantener la información almacenada).
- **Unidad central de procesamiento (CPU):** También denominada *procesador* es el elemento encargado del control y ejecución de las operaciones del sistema. Se puede considerar como el cerebro del ordenador y está compuesto, a su vez de dos unidades:
  - **La unidad de control:** Es el elemento encargado de coordinar todas las actividades de la computadora. Para ello, se comunica con todas las demás unidades e interpreta y ejecuta ordenadamente las instrucciones del programa en curso.
  - **La unidad aritmética-lógica (ALU)**: Está constituida por los circuitos electrónicos necesarios para la realización de operaciones elementales de tipo aritmético (suma, resta, multiplicación, división, etc.) y lógico (comparación, operación OR, AND, XOR, INV, NOR, NAND, etc.).

2.7.1 Unidades de entrada

Son aquellos dispositivos encargados de aceptar datos de entrada e instrucciones del exterior y transformarlos en señales binarias eléctricas susceptibles de ser procesadas directamente por el ordenador. Ejemplos típicos de entrada son el teclado y el ratón (Mouse).

2.7.2 Unidades de Salida

Son aquellos dispositivos que devuelven al exterior datos de salida obtenidos como resultado de algún tipo de procesamiento. Se encarga de transformar las señales a un formato comprensible por el humano (gráficos, sonido, etc.). Ejemplos típicos de unidades de salida son los monitores y las impresoras.

2.7.3 Memoria Masiva o Auxiliar

Está formada por aquellos dispositivos de almacenamiento masivo de información, utilizados para guardar datos e instrucciones para su posterior uso en el sistema informático. Frente a la memoria principal, este tipo de memorias se caracterizan por su gran capacidad de almacenamiento y por ser no volátiles (al igual que las memorias ROM, son memorias permanentes). Gracias a estos elementos, se consigue retener la información introducida en el sistema informático, sin tener que introducirla nuevamente. Este tipo de unidades integran generalmente un dispositivo de lectura/escritura de información, así como un soporte de almacenamiento (disco, cinta, etc.). Ejemplos típicos de unidades de memoria masiva son los discos rígidos (discos duros), los lectores de CD-ROM, las unidades de disco flexible (disquetes), unidades ZIP y las memorias USB (128MB, 256MB y 1GB). También se hace referencia a este tipo de memorias con el nombre de *memoria secundaria o memoria externa.*

La computadora central dispone dentro de sus unidades de elementos adicionales de memorización con muy baja capacidad. Estos elementos, a diferencia de la memoria principal, sirven para retener temporalmente pequeñas cantidades de información (una palabra o un byte) y se denominan **registros**. Así, por ejemplo se utiliza un registro para almacenar temporalmente la dirección de memoria principal cuyo contenido va a ser leído en un momento determinado.

Debido a su disposición, todas las unidades externas a la computadora central, es decir, las unidades de entrada, las unidades de salida y las unidades de memoria masiva, son denominadas genéricamente con el nombre de **periféricos.** También es importante incluir dentro de los principales elementos Hardware, determinados elementos adaptadores que hacen posible una comunicación eficaz entre dos unidades y que reciben el nombre de **interfaces** (por ejemplo, una interfaz entre una impresora y una CPU). El término interfaz no sólo se utiliza en el campo del hardware, sino que puede hacer referencia a elementos software. Así, por ejemplo, existen programas que funcionan como interfaces entre usuarios y otro programa, haciendo más sencillo el uso de dicho programa; a este tipo de interfaz se le da el nombre de *interfaz de usuario.*

2.8 Factores que influyen en la potencia de una computadora

La potencia o poder de cómputo de una computadora generalmente hace referencia a la velocidad con la cual dicha computadora procesa los datos. Por consiguiente, cuando más potente sea una computadora, el procesamiento será llevado a cabo más rápidamente. Existen determinadas características de una computadora que permiten cuantificar su potencia. Aquí citaremos los factores más importantes que influyen en la potencia de una computadora:

- **La frecuencia del reloj interno de la computadora**: Dentro de la unidad de control, existe un dispositivo denominado *reloj o generador de pulsos* que sincroniza todas las operaciones elementales de la computadora. Este reloj funciona a una frecuencia constante del orden de millones de veces por segundo. Evidentemente, cuanto mayor sea la frecuencia de reloj de una computadora, mayor número de operaciones podrá realizar por unidad de tiempo. Este parámetro se mide generalmente en millones de ciclo por segundo (Megahertzios, MHZ).

- **El ancho de banda**: Representa la cantidad de información transferida por segundo de una unidad funcional a otra (se mide en Megabytes por segundo, MB/s). Cuando mayor sea el ancho de banda entre dos unidades, más rápido será el intercambio de información entre ambos, y esto influirá muy positivamente en la velocidad de cómputo.

- **La longitud de palabra**: Dentro de la computadora central se trabaja con unidades de información superiores al byte, las palabras. Una *palabra* equivale a un número entero de bytes y representa la cantidad de información que se transfiere en un instante dado entre las unidades de la computadora central. La *longitud de palabra* es el número de bits que forman una palabra. Cuanto mayor es la longitud de palabra de un ordenador, éste podrá operar en cada instante con datos que ocupen mayor número de bits, por lo cual las operaciones sobre datos complejos (como pueden ser vectores) podrán ser realizadas a mayor velocidad. Hoy en día, lo más usual es encontrar computadoras con una longitud de palabra de 32 bits.

- **La capacidad de memoria principal:** Cuando mayor sea el tamaño de la memoria RAM de una computadora, ésta podrá ejecutar programa más grandes y que necesiten procesar mayor cantidad de datos. Por otro lado , no es necesario que una computadora cargue un programa completo en su memoria para ejecutarlo, pero cuanto mayor sea la memoria RAM, menos accesos a memoria masiva serán necesarios (para poder intercambiar parte del programa entre memoria principal y memoria masiva), y como consecuencia, el programa será ejecutado más rápidamente.

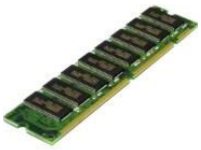
A esta organización por bloques o módulos que dependen y se conectan a un bloque principal (la tarjeta madre), se le conoce como arquitectura modular, concepto que toma forma a nivel de estándar con el modelo PC de IBM, según explicare más adelante.

2.9 Placa Madre, Placa Base o Tarjeta Madre

También se la llama placa principal y es el circuito impreso que permite la unión de todos los componentes. Por ella circulan toda la información procesada por la CPU. En la placa, entre otras cosas, se encuentran las siguientes partes:

- ***Compartimiento para el microprocesador***, que es el lugar donde se instala el microprocesador, dependiendo del tipo de chip tendrá una forma u otra. Las dos técnicas básicas de anclaje son zócalo y spot o ranura.
- ***Chisep y/o controlador de discos***. Algunos modelos cuentan con este circuito que le permite la instalación de discos IDE o SCSI, dependiendo del circuito que vengan con su placa base. Normalmente cuenta con tres conectores, dos de los cuales son de 40 pines en los cuales se conectan las unidades de disco duro y CD-ROM. Sólo es posible instalar dos unidades por cada conector. Hay otro conector de similares características pero un poco más pequeño, de 32 pines, en el que va conectada la unidad de disquete.
- ***Ranura AGP*** (las viejas no la tienen). Es una ranura, normalmente de color marrón, en la cual se inserta la tarjeta gráfica arquitectura AGP.
- ***Ranuras de expansión***. Son de formato parecido a la ranura AGP, las hay de dos tipos ISA y PCI. Las ISA son más grandes y las placas actuales sólo cuentan con una o dos. Suelen ser de color negro. Las PCI son algo más pequeñas y habitualmente de color blanco. En ellas se colocan las tarjetas de expansión (tarjetas de video o de sonido, placa de red, etc.). La diferencia funcional entre ISA y PCI es que estas últimas trabajan con 64 bits, mientras que las primeras lo hacen con 16, además, las ranuras PCI son autoconfigurables (plug and play) y las ISA necesitan configuración manual.
- ***Zócalos de memoria***. Sobre estas ranuras se instalan los módulos de memoria RAM. Dependiendo de la velocidad de la placa 100, 133Mhz, etc. Se podrá instalar memoria de un tipo u otro. Las memorias de 133Mhz funcionan en las placas de 100 Mhz pero no al contrario.
- ***Conectores para periféricos***. Estos conectores responden a estándares internacionales que permiten el reemplazo de diferentes placas,
- Otros componentes. En la placa madre existe gran cantidad de componentes que iremos describiendo en el capítulo escrito para tal fin, pero no podemos dejar de mencionar a la memoria BIOS que es la encargada de hacer “arrancar “al microprocesador para la computadora cargue el sistema operativo que le permita funcionar.

2.10 Memoria RAM



Es la encargada de almacenar los datos y programas que se están utilizando en cada momento mientras la computadora está encendida. El usuario no tiene control real sobre la memoria ya que su administración es función del sistema operativo.

La memoria es un espacio de almacenamiento temporal gestionado por el microprocesador. Los datos contenidos en ella desaparecen cada vez que se apaga el equipo, a diferencia de

lo que ocurre con el disco rígido en el cual la información almacenada es gestionada por el usuario y permanece por más que se quite la alimentación a la computadora.

Las memorias se disponen en “barras” o módulos que contiene una serie de chips y van encajados perpendicularmente en los zócalos o bases de la placa madre. Hay varios tipos de memoria y no todos son compatibles con todas las placas.

2.11 Fuente de Poder

Es la encargada de suministrar las diferentes tensiones para el funcionamiento de los elementos conectados a la placa madre (2.8v, 3v, 12v, 15v, etc.). La fuente de alimentación tiene un conector en la cara que asoma por la parte posterior del PC para enchufar el cable de alimentación y un interruptor que permite encender o apagar totalmente el equipo. El cable que sale de la fuente que tiene el conector más grande, con dos hileras de 10 pines cada una, se conecta a la placa base. Los otros conectores alimentan a las diferentes unidades de disco: disco duro, DC, DVD, disquetera, etc.

Una computadora debe protegerse de la corriente eléctrica externa, surtiéndose de una fuente de alimentación estable y constante y protegiéndose con aparatos que ejerzan la función de barrera tales como los reguladores de voltaje y supresores de picos. La instalación de un polo a tierra física, atenúa el daño de una sobrecarga o cortocircuito, derivando el exceso de corriente hacia el exterior del sistema, y protegiendo al operador.

El circuito eléctrico de alimentación de una computadora (alimentación de la fuente) necesita normalmente tres líneas de alimentación: La Fase, El Neutro y La Tierra Física. En la secuencia de instalación se conecta primero el regulador de voltaje o un no break quien se encarga de mantener un voltaje promedio (110-115Volts o 210-220Volts, según la tensión de la red). Un buen regulador interrumpe el circuito de alimentación cuando las variaciones de tensión exceden los rangos en un 20%.

En ciertos casos, es necesario instalar a continuación una fuente de energía ininterrumpida o UPS (No-Break’s), en la actualidad existen No-break’s que tiene integrados reguladores de voltaje, esto es cuando trabajamos con datos valiosos o delicados en el PC. Después del regulador o UPS se conecta la computadora.

2.12 Disco Rígido o Disco Duro

INTERIOR DISCO DURO

Es la unidad fija de almacenamiento. Aquí se guardan los programas, los datos y el sistema operativo (Windows, Linux, Unix, etc.). La capacidad del disco duro se mide en Gigabytes (antes era en Megabytes) y cualquier programa que instala ocupa parte de estos Gigabytes.

Dentro de una computadora puede haber varios discos duros, incluso un disco duro se puede particionar y el sistema lo reconoce como un disco duro diferente. En la parte posterior del disco se encuentran todos los conectores y puentes para su configuración. El conector de suministro de corriente es rectangular, de unos dos centímetros de largo y con dos vértices oblicuos (con chanfle). Cualquiera de los grupos de cables que salen de la fuente con un conector que encaje en dicho enchufe sirve para alimentar al disco. El conector de datos también es rectangular y tiene dos hileras de pines con un total de 40 (IDE). Se utiliza un

cable plano para unir el disco duro desde este conector con uno similar que hay en la placa base o tarjeta controladora. Por último, hay un grupo de puentes (jumpers) que permiten la configuración del disco, es decir, su nivel de prioridad dentro del controlador. Algunas combinaciones posibles para la configuración son:

MA: Master. Establece que es el único disco del cable o bien el definido como principal.
SL: Slave. Segundo disco del cable
CS: Cable Select (selección por cable). En función del conector del cable en el que está el disco, puede ser maestro o esclavo.

2.13 Unidades de CD/DVD/CDRW

LECTOR DE DVD

En principio son la unidades definidas como multimedia que poseen en la parte posterior conectores similares a los descritos para el disco duro, agregándole un conector más, que a su vez es más pequeño con una sola hilera de pines para la salida de audio, desde la cual parte un cable que va a la entrada de CD situada en la tarjeta de sonido.

Existen lectores, grabadores y regrabadores. Los más flexibles son los últimos, ya que permiten trabajar en 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.

2.14 Unidades extraíbles (unidades ZIP)

La unidad ZIP es una unidad de disco extraíble, portátil, barata, y de moda. Sus discos tienen una capacidad de 96 MB, y las unidades están disponibles en dos versiones, una versión SCSI y una versión para puerto paralelo que es la más fácil y más rápida de configurar y de instalar.

Unidad ZIP.

2.15 Unidad de disquete 3 ½ pulgadas

Es la encargada de leer y grabar disquetes. Al igual que los otros tipos de unidades, tiene un pequeño conector de datos con 32 pines en lugar de 40 y uno de alimentación que es un poco más pequeño. Las conexiones son similares a lo visto recién.
El cable de la disquetera lleva un cruce entre los dos juegos de

conectores, que identifican la unidad A y la B. Si la disquetera está conectada después del cruce, será la unidad A; de lo contrario será la B. En algunos sistemas se puede asignar la letra de la unidad a través del BIOS de la máquina.

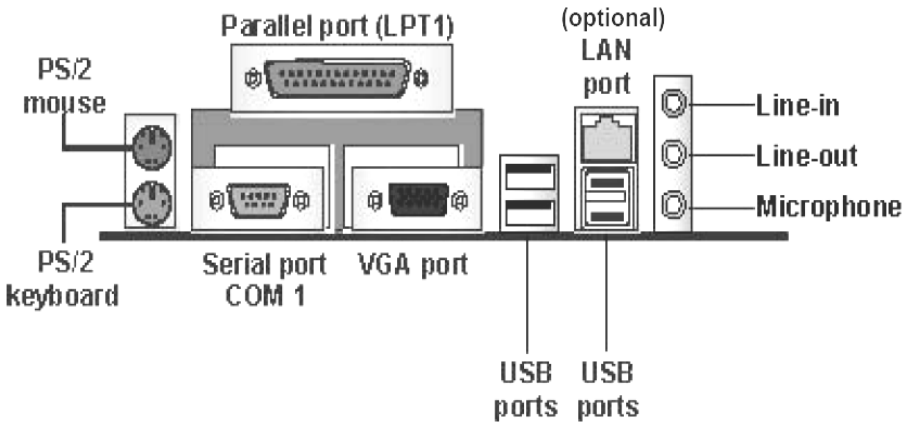
2.16 Tarjeta Gráfica

Es la comúnmente llamada placa de video y puede estar instalada en la ranura AGP o en uno de los conectores PCI, dependiendo de la arquitectura de la tarjeta. Es la encargada de transmitir los datos al monitor para su visualización. Por la parte exterior de la caja de la computadora sale el cable de datos que va al monitor.

2.17 Tarjeta de Sonido

Se la conecta en una ranura PCI o ISA. En la parte exterior del gabinete de la computadora estarán presentes una serie de conectores que varían en función de las marcas y modelos de estas tarjetas. Sin embargo, todas tienen un conector para parlantes (altavoces o bocinas) o auriculares, otro para micrófono y un tercero de entrada de línea para grabar sonido procedente de cualquier equipo de música.

En la placa hay lugar para un conector que la une con la unidad de CD, que se utiliza para reproducir discos compactos. En él se conecta un cable que viene desde la salida de audio de la unidad de CD/DVD/CD-RW.



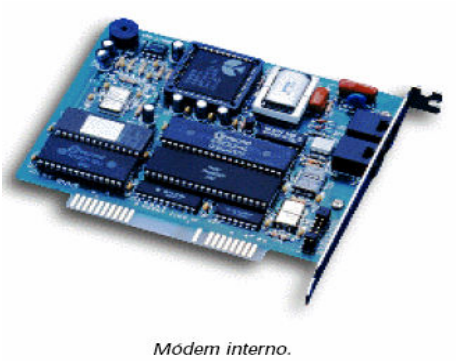
2.18 Módem (Modulador Demodulador)

Este dispositivo permite interaccionar a la PC con una línea telefónica, ya sea para poder enviar un fax o poder conectarse a Internet, existen principalmente dos tipos de módem: módem interno y el externo.

a) Módem interno

Éste va insertado en la ranura de expansión de la PC, es una tarjeta, tiene dos conectores, en uno se conecta la línea telefónica y en el otro el teléfono, utiliza software de comunicaciones.

Módem externo.



Módem interno.

b) Módem externo

Es un dispositivo externo, generalmente de forma rectangular, que se coloca en el exterior de la PC, se conecta a través del puerto serial y utiliza un software de comunicaciones.

2.19 Tarjeta de red

Este dispositivo se utiliza para redes LAN (Local Area Network), existen diversos tipos de tarjetas de red, sin embargo la finalidad es la misma, conectar computadoras en red.

Tarjetas para red.

2.20 Monitores

El monitor es el principal dispositivo periférico de salida de datos, sin embargo no se le pone mucha importancia, hay que tener en cuenta que junto con el teclado y el ratón son las partes que interaccionan con nuestro cuerpo, y que si no le prestamos la atención debida, podremos llegar incluso a perjudicar nuestra salud.

2.20.1 Tipos de monitores

Existe una gran variedad de monitores, ya sea en tamaño, diseño, marcas y precios, hay monitores monocromáticos (fondo negro y letras verdes, ambar, etc.) y monitores que pueden desplegar un sinfín de colores y matices, a continuación se explican brevemente algunos tipos de monitores.

- *HÉRCULES*

Es un estándar de exhibición de video para PCs, de *Hercules Computer Tecnology Inc*., que provee gráficos monocromáticos y texto con una resolución de 720 x 348 Pixeles. Hoy en día, se les puede ver en bancos o supermercados, son muy comunes para este tipo de empleos ya que se pasan largas horas trabajando frente a este tipo de monitores, esto evita que se canse la vista y se tengan dolores de cabeza.

- *CGA (Color/Graphics Adapter)*

Es un estándar de gráficos/color, una presentación de video de IBM que provee texto y gráficos de baja resolución.

- *EGA (Enhanced Graphics Adapter)*

Estándar de exhibición de video de IBM que provee textos y gráficos de resolución media

- *VGA (Video Graphics Array)*

Es un estándar de presentación de video de IBM, que se ha incorporado a los modelos más sofisticados de la serie PS/2 de IBM, suministra textos y gráficos de media a alta resolución, soporta estándares de presentación previos, tiene 16 colores en su máximo modo gráfico (640 x 480).

- *SVGA (Super Video Graphics Array)*

Es un estándar de video de IBM que presenta hasta 256 colores, y tiene un modo de resolución mucho más alta y mejorada de 800 x 600 pixeles.

- *UVGA (Ultra Video Graphics Array)*

Son los monitores más modernos que existen en el mercado, tienen la mejor resolución de video y por lo mismo son los más aceptados por los usuarios ya que permite un mejor despliegue de textos y gráficos para juegos en 3D.

- *MULTISYNC*

Es un monitor que se adapta automáticamente a la frecuencia de sincronización de la señal de video que recibe, puede adaptarse a un rango de frecuencias. Fue popularizado por NEC y Multisync es el nombre comercial, es muy raro encontrarse actualmente con este tipo de monitores.

2.20.2 Características

A continuación se explicará brevemente los parámetros o características que influyen en la calidad de un monitor:

- *Tamaño*

El tamaño se mide en pulgadas y lo que se mide es la longitud de la diagonal, el tamaño es importante porque permite tener varias tareas a la vez de forma visible y poder trabajar de forma más cómoda, el tamaño mínimo aconsejable es de 14 pulgadas.

- *Tubo*

El tubo nos definirá si la pantalla es más o menos plana y cuadrada, el tamaño del punto (Dot Pix) y también servirá para comparar entre diferentes marcas por si hay un posible daño, como por ejemplo que se dañe el Flash Back, los controles de brillo y contraste, entre otros.

- *Tamaño del punto*

Esta característica depende del tubo y define el tamaño que tendrá cada uno de los puntos que forman la imagen, entre más pequeño más preciso será. No hay que confundir el tamaño del punto con el pixel, ya que el pixel depende de la resolución de la pantalla y puede variar.

- *Frecuencia de refresco*

Se refiere a que la frecuencia tiene que ser lo suficientemente alta para que el barrido de la imagen no se distorsione, la frecuencia está proporcionalmente ligada a la estabilidad de la imagen y por tanto al confort y descanso de la vista.

- *Resolución*

Se denomina como la cantidad de pixeles* que se pueden ubicar en un determinado modo de pantalla, los *pixeles están distribuidos entre el total de horizontales y verticales de la pantalla.

*Pixel (picture element).- Es el elemento más pequeño en una pantalla de presentación de video. Una pantalla se divide en miles de pequeños puntos, y un pixel es uno o más puntos que se tratan como una unidad, un pixel puede ser un punto en una pantalla monocromática, tres puntos (rojo, verde, azul) en pantallas de color.

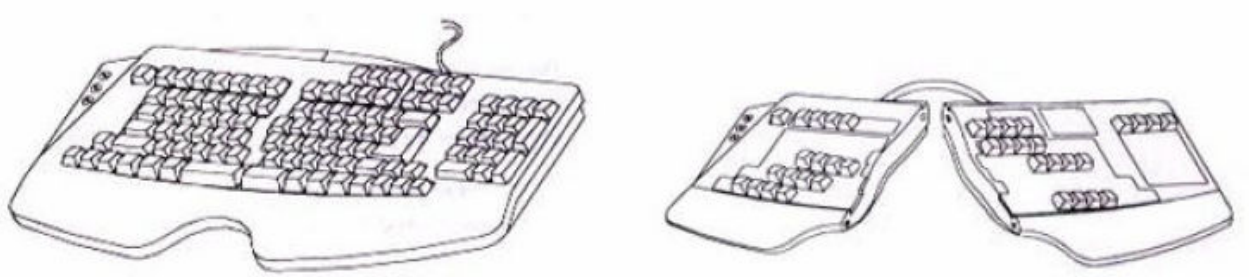
- *Conector*

En ambientes domésticos y de oficina es común encontrarse con el conector DB15, pero en entornos especializados donde se cuenta con monitores grandes y de mayor calidad se necesitan conectores BNC, ya que ofrecen una mayor protección frente a interferencias.

Monitor SuperVGA.

2.21 Teclado

Este es el principal dispositivo periférico de entrada que se divide en tres partes: teclado numérico, teclas de función y teclado alfanumérico, además de un cierto número de teclas especiales; asimismo existen dos estándares de interfaz para el teclado, que son DIN y Mini-DIN, hay diversos tipos de teclados, los hay muy modernos como los ergonómicos, para Windows 95 o 98, inalámbricos, etcétera.



Teclados ergonómicos.

2.21.1 Interfaz del teclado

El teclado como todos los dispositivos necesita de una interfaz que lo comunique con el resto de la computadora, para ello cuenta con un conector; existen dos estándares de conectores para teclado, éstos son:

- *DIN*

El cable del teclado corre de un conector DIN, tiene 5 patas (no en orden numérico consecutivo).

- *Mini-DIN*

Este tipo de conector fue introducido por IBM y utilizado en equipos de "marca", y es el habitual en las placas con formato ATX, tiene el mismo formato que el DIN pero el conector es más pequeño.

Ratón.

Interfaz del teclado.

2.22 Ratón (Mouse)

Es un dispositivo que se usa como puntero o marcador. A medida que se hace rodar sobre el escritorio en cualquier dirección, el cursor o puntero se mueve correspondientemente sobre la pantalla.

Hay dos tipos de ratón: ratón mecánico-óptico y ratón óptico.

- *Ratón mecánico – óptico*

Es un ratón que utiliza una pelota de goma que hace contacto con varias ruedas dentro de la unidad, las cuales al girar interrumpen señales infrarrojas que determinan su posición.

- *Ratón óptico*

Utiliza la luz para obtener sus coordenadas. Es desplazado sobre una pequeña tableta que contiene una rejilla reflejante, colocada sobre el escritorio. El ratón emite una luz y capta su reflexión a medida que se desplaza.

CAPITULO 3
EL ELEMENTO LÓGICO: EL SOFTWARE

3.1 Introducción

Recordemos que el **software** era la parte lógica e inmaterial de un sistema informático que proporciona al hardware la capacidad para realizar determinadas tareas. En definitiva, el software estaría formado por un conjunto de programas ejecutables en una computadora, así como de los datos y documentos asociados a dichos programas. Generalmente, el software como elemento lógico es almacenado en soportes físicos, como son la memoria principal, la memoria masiva, el papel impreso, etc.

Antiguamente, los equipos físicos (es decir, el hardware) eran caros y difíciles de usar, mientras que el software se veía como un añadido. Con el paso del tiempo, esta situación ha ido cambiando, el software ha ido adquiriendo más peso específico conforme los costes del hardware se iba reduciendo, de tal forma que en la actualidad el software tiene más importancia en todos los aspectos (coste, mantenimiento, etc.) que el hardware.

3.2 Esquema Básico del Software

Teniendo en cuenta que el concepto de software está íntimamente ligado al concepto de programa, analizaremos con mayor detalle la definición de programa. Un **programa** no es más que un conjunto ordenado de instrucciones que se le dan a la computadora para indicarle la tarea que se desea realizar. Aquí, una **instrucción** es un conjunto de símbolos de un repertorio, construidos de acuerdo a unas reglas, que representan una orden de operación para la computadora. Las instrucciones de un programa responden a unas reglas sintácticas y semánticas bien establecidas que definen lo que se denomina un **lenguaje de programación**.

Existen muchos tipos de lenguajes de programación, pero cada modelo de computadora sólo es capaz de entender directamente un determinado lenguaje. Se denomina **lenguaje máquina** de un ordenador concreto al conjunto de reglas y símbolos necesarios para construir instrucciones directamente interpretables por los circuitos electrónicos de la unidad de control de dicho ordenador. La construcción de programas en lenguaje máquina resultan muy laboriosa, ya que las instrucciones se representan sólo con números (en código binario), existen muy pocas instrucciones y es necesario conocer perfectamente las características hardware del modelo de computadora (existe una gran dependencia de la máquina).

Para subsanar los problemas que conlleva la programación en lenguaje máquina, se han desarrollado lenguajes más cercanos al hombre: los **lenguajes de alto nivel**. Estos lenguajes se caracterizan fundamentalmente porque son independientes del modelo de computadora y por otras cualidades orientadas a hacer más fácil y directa la labor del programador. Ejemplos bastante conocidos de lenguajes de alto nivel son: COBOL, C, C++, PASCAL, BASIC, PROLOG, ADA, JAVA, FOX PRO, etc.

Naturalmente, teniendo en cuenta que una computadora sólo entiende el lenguaje máquina, serán necesarios determinados elementos capaces de traducir un programa escrito en un lenguaje de alto nivel al lenguaje máquina de un ordenador concreto. Estos

elementos serán otros programas denominados **traductores**, los cuales harán posible la ejecución de programas en un lenguaje de alto nivel concreto sobre un tipo de ordenador específico. Dependiendo de cómo se realice el proceso de traducción, existen dos tipos de traductores: los compiladores y los intérpretes. Los **compiladores** traducen globalmente el programa inicial (programa fuente), obteniendo un programa semánticamente equivalente en lenguaje máquina (programa objeto) que será ejecutado después de la traducción. Los **intérpretes** analizan, traducen y ejecutan las instrucciones del programa fuente secuencialmente, de tal forma que la traducción y la ejecución del programa fuente se entrelazan en el tiempo. En este último caso, no se genera un programa objeto como salida, sino que los resultados de la ejecución del programa son generados directamente.

Para que una computadora pueda funcionar, es necesario disponer de una serie de programas (generalmente proporcionados por la firma constructora de la computadora) necesarios para el control del mismo y su utilización eficiente y cómoda por parte del usuario. Este conjunto de programas conforman el software más básico del sistema, que recibe el nombre de **sistema operativo.** El sistema operativo es un conjunto de programas y funciones que controlan y gestionan el funcionamiento del hardware, ocultando sus detalles al usuario, con dos objetivos principales:

1. Alcanzar un eficaz rendimiento de los recursos hardware (memoria, periféricos, CPU, etc.) del sistema informático y
2. Facilitar al usuario un acceso flexible y sencillo a dichos recursos, es decir hacer transparente al usuario las peculiaridades propias de cada recurso.

En la actualidad, los sistemas operativos del momento ofrecen a los usuarios grandes posibilidades, como son el uso del sistema informático por varios usuarios simultáneamente (sistemas operativos multiusuario), la distribución de los recursos del sistema informático sobre redes de ordenadores (sistemas operativos distribuidos), sofisticadas interfaces de usuario basadas en gráficos, ventanas, iconos, etc. Actualmente los sistemas operativos más conocidos son UNIX, LINUX, SOLARIS, WINDOWS NT, OS/2, el sistema operativo de Macintosh y WINDOWS (3.1, 95, 98, 98 SE, MILENIUM, XP Y 2003).

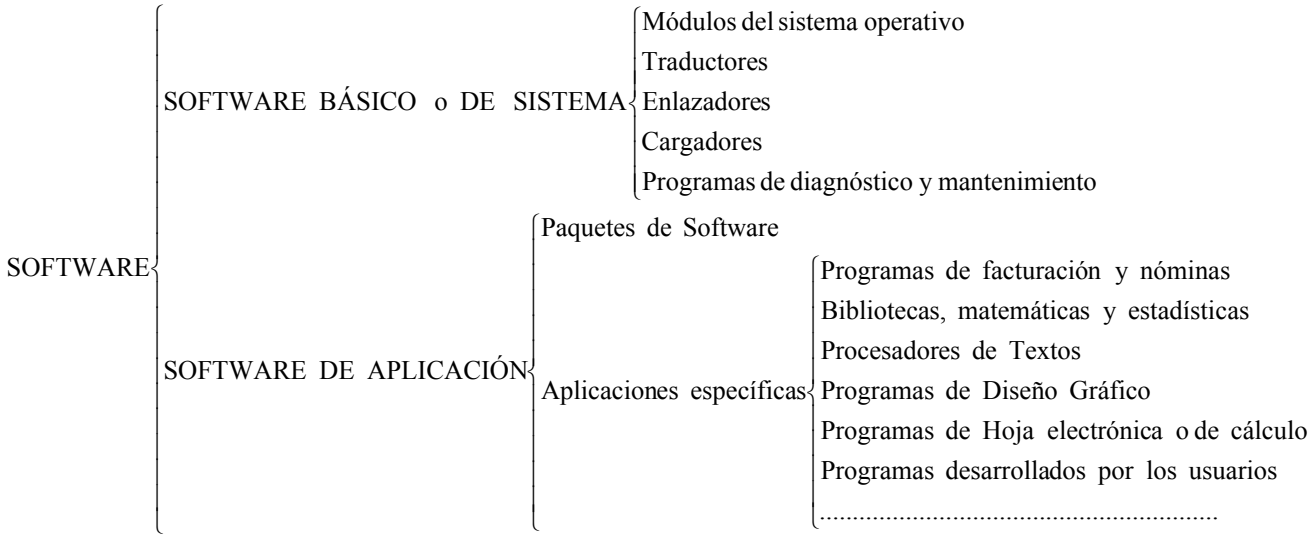


Figura 3.1 Esquema básico del software de un sistema informático

Hasta el momento, sólo hemos hablado de dos tipos de software, el software de traducción o traductores y el software de sistema operativo. Estos dos tipos forman parte de un grupo más general, denominado software básico o de sistema. El **software de sistema** está compuesto de aquellos programas necesarios para el funcionamiento de la computadora, junto a un conjunto de programas orientados a facilitar el uso del sistema y optimizar sus recursos.

Además del software del sistema, deben existir programas especialmente diseñados para realizar trabajos concretos o para aplicaciones específicas. A este tipo de software se le denomina **software de aplicación.** Dentro del software de aplicación, podemos destacar por su importancia:

- **Los paquetes de Software:** Compuestos de una serie de programas que permiten editar textos, almacenar y gestionar datos, realizar cálculos, generar informes, comunicarnos con otros ordenadores, enviar y recibir correo, etc.
- **Las aplicaciones de uso específico:** Facturación, contabilidad, nóminas, etc.

3.3 Organización de los Datos

Los datos utilizados por los programas forman parte del software. Estos datos suelen almacenarse en memoria masiva hasta que parte de los mismos son requeridos por un programa en ejecución. En este apartado, expondremos algunos conceptos y definiciones básicos acerca de cómo se organizan los datos en memoria masiva.

Si bien los datos se almacenan en memoria masiva según una estructura física, el sistema operativo permite que el usuario trabaje con una estructura lógica que resulta mucho más fácil de comprender. Esta estructura lógica está basada en ficheros que constituyen la herencia de los sistemas manuales de tratamiento de datos basados en ficheros manuales (en archivadores).

Un **fichero** es un concepto lógico que representa un conjunto de información del mismo tipo referente a unos determinados datos, tratada como una unidad de almacenamiento y organizada de forma estructurada para la recuperación de un dato individual. Ejemplos: fichero de empleados de una compañía, de alumnos de una facultad, de libros en una biblioteca, etc. Los datos que lee o genera un programa suelen estructurarse en forma de ficheros de datos. Los ficheros de datos de entrada a un programa pueden ser introducidos en la memoria masiva antes de la ejecución del programa que los procesa.

La unidad elemental que compone los ficheros es el registro. Un **registro** equivaldría a una ficha en un fichero manual, es decir, contendría la información correspondiente a cada elemento individual. Así, por ejemplo, en un fichero de empleados, los datos referentes a un empleado concreto formarían un registro del fichero.

A su vez, cada registro de un fichero se compone de unidades más simples denominadas campos. Un **campo** representa una información unitaria e independiente dentro de un registro. Ejemplo: Nombre_empleado, Título_Libro, Nota_Alumno, etc. Cada campo, a su vez, se compone de caracteres (cada uno ocupando un byte).

La forma más común de identificar un registro dentro de un fichero es elegido un campo, o conjunto de campos, dentro del mismo para el cual cada registro mantenga

diferentes valores. A este campo o conjunto de campos se le denomina **llave**. En la figura siguiente se muestra el contenido de un fichero de empleados en el cual el campo NIF_*empleado* podría actuar como llave.

Campo				
Nombre_empleado	**NIF_empleado**	**Fecha_comienzo**	**Categoría**	
Pedro García Ríos	56.675.867-H	13-12-95	A	
Alfonso Ramirez	45.456.234-I	02-02-96	B	**Registro**
María López	12.234.345-O	05-23-96	B	
Rosa Rojas Ruiz	23.423.456-L	09-04-95	D	

Figura Estructura de un fichero para almacenar información acerca de los empleados de una compañía

La mayoría de las organizaciones que emplean ordenadores, lo hacen para más de un propósito; es decir, una misma empresa puede mantener diferentes aplicaciones que utilicen los mismos datos. Cada una de las aplicaciones requiere un gran volumen de datos, utilizándose ficheros para almacenarlos (en memoria masiva). Cada aplicación podría disponer de su propio conjunto de ficheros que contuvieran los datos que necesite estructurados adecuadamente. Debido a que los datos son para una misma compañía, existe un alto grado de solape entre los datos para las distintas aplicaciones. Así, por ejemplo, si la sección de personal de una compañía mantiene un fichero de empleados y la sección de contabilidad también necesita otro fichero para almacenar información de los empleados, existirán información duplicada.

El enfoque anterior presenta problemas al existir información común a varios ficheros (duplicidad). Esta duplicidad lleva consigo las siguientes desventajas: mayor trabajo de introducción de datos, depuración de errores más complicada, mayor ocupación de memoria masiva, problemas de actualización, etc.

Para resolver el problema, se reemplazan todos los ficheros por una única colección de ficheros interconectados lógicamente, generalmente de gran tamaño, accesible por todas las aplicaciones, es decir, por una **base de datos**. Generalmente, esta estructura se construye de acuerdo a la organización global de la empresa y a sus necesidades, no dependiendo de ningún programa concreto que haga uso de dichos datos. Las bases de datos se crean, actualizan y utilizan mediante programas especiales denominados **gestores de bases de dato.** Los gestores de bases de datos permiten, entre otras acciones, definir la estructura lógica de una base de datos y realizar operaciones de mantenimiento, modificación y consulta sobre una base de datos previamente existente.

3.4 La Memoria BIOS

Cuando encendemos la PC, el sistema operativo se encuentra en el disco duro o bien en un disquete, pero: ¿cómo sabe el µP que tiene un disco duro o una disquetera?, ¿cómo y dónde guarda esos datos, junto con el tipo de memoria y de caché o la fecha y la hora?

Pues para todo esto está la BIOS. La BIOS (Basic Input Output System, Sistema de entrada/salida básico) es una memoria ROM, EPROM o FLASH-RAM a la que se le introducen las rutinas de bajo nivel que permiten que la CPU pueda arrancar, controlando el teclado el disco duro y la disquetera para luego ejecutar el sistema operativo.

La BIOS también contiene el programa de configuración que muestra los menús y pantallas que aparecen cuando accedemos a los parámetros del sistema, pulsando una o varias teclas durante el proceso de inicialización de la máquina.

La BIOS trabaja en conjunto con la denominada memoria CMOS (llamada así porque suele estar hecha de esta tecnología, por lo que muchas veces el programa que modifica la BIOS se denomina **"CMOS Setup"**), que almacena los datos propios de la configuración del microprocesador, ya sean los discos duros que tenemos instalados con el número de cabezas y cilindros, el número y tipo de disqueteras, la fecha y hora real y otros datos necesarios para el correcto funcionamiento de la computadora. La BIOS se alimenta por una batería (dura años debido al bajo consumo de estas memorias), de modo que, cuando apaguemos la computadora no se pierdan todos esos datos que precisa la CPU para funcionar. La BIOS se aloja en la placa base, cerca de la pila que es de tipo botón y suele durar 4 ó 5 años y es muy fácil de reemplazar. Las primeras placas traían la pila soldada, lo que dificultaba el cambio, además de otros problemas como que la pila tuviera pérdidas y se sulfatara ésta y la placa.

Para cambiar la pila, apunte todos los datos de la BIOS, desconecte todo y sustitúyala por una igual, o bien por un paquete externo de baterías que se conectan a un jumper (un microinterruptor) de la placa base; ambas cosas las debería en una casa de electrónica.
Después conecte todo, arranque la computadora, entre al BIOS y reintroduzca todos los datos, ya que se habrán borrado.

La BIOS es la responsable de la mayoría de los mensajes que surgen al encender la computadora, justo antes del "Indicado MS-DOS" o bien Windows 95, Windows 98, Windows 2000, Windows Milenium o Windows XP, Linux, OS/2 o lo que sea. La secuencia típica en que aparecen esos mensajes suelen ser:

- Primero los mensajes de la BIOS de la tarjeta gráfica (esta tarjeta tiene su propia BIOS).
- El nombre del fabricante de la BIOS y el número de versión.
- El tipo de microprocesador y su velocidad.
- La revisión de la memoria RAM y su tamaño.
- Cómo acceder a la BIOS ("Press DEL to enter CMOS SETUP", por ejemplo).
- Mensajes de otros dispositivos, habitualmente del disco duro, teclado o mouse, etc.

Al conjunto de esos mensajes se le denomina POST (Power-On Self Test, literalmente auto-prueba de encendido), y sirve para verificar que no existen mensajes de error, para ver si la cantidad de memoria corresponde a la que debería y para averiguar cómo se entra en la BIOS. Generalmente se hará mediante la ejecución de ciertas teclas al arrancar, mientras salen esos mensajes. Uno de los métodos más comunes es pulsar "DEL o SUPR", aunque en otras se usa "F1", "Esc" u otra combinación de teclas (Alt-Esc, Alt-F1, etc.). Si desea información general sobre estos mensajes puede remitirse a su Manual de Usuario, sino lo tiene lo puede buscar en Internet dirigiéndose a la página del fabricante y buscar el modelo de la Placa base que a veces lo traen impreso en la misma.

3.5 Manejo de la BIOS

Las BIOS clásicas se manejan con el teclado, típicamente con los cursores y las teclas de "Enter", "Esc", la barra espaciadora y las teclas de direcciones (←↑→↓), aunque también existen BIOS gráficas, las llamadas WinBIOS, que se manejan con el mouse en un entorno de ventanas.

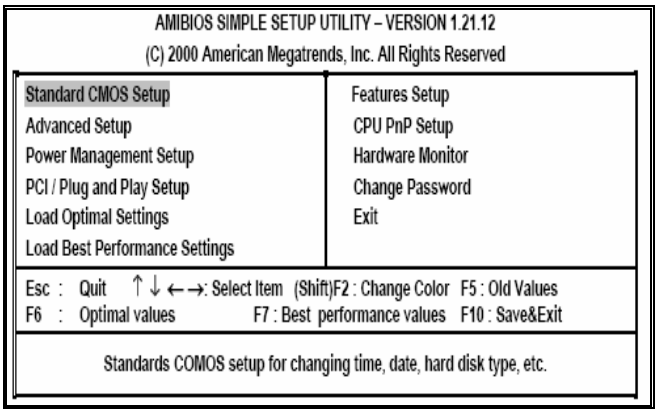


Fig. 3.3 BIOS Clásico

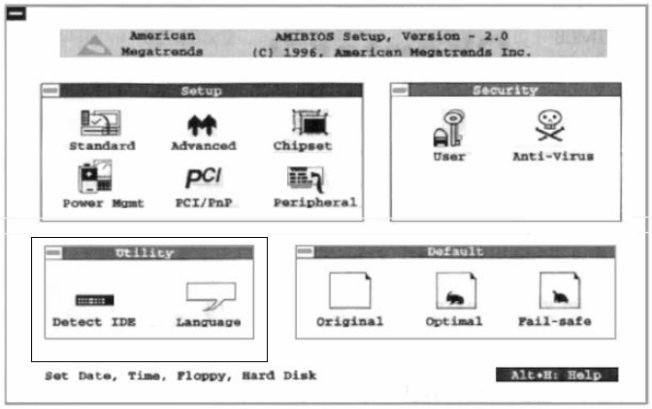


Fig. 3.4 WINBIOS

Existen varios ítems comunes a todas las BIOS que son:

Configuración Básica, llamado generalmente "Standard CMOS Setup" o bien Standard Setup".
Opciones de la BIOS, llamado "BIOS Features Setup" o "Advanced Setup".
Configuración avanzada y del chipset, "Chipset Featuares Setup".
Otras utilidades, autoconfiguración de la BIOS, manejo de PCI, introducción de contraseñas – passwords, autodetección de discos duros, etc. Para salir de un menú se suele usar la tecla "Esc", además, ningún cambio queda grabado hasta que no se lo indicamos al ordenador al salir de la BIOS.

3.5.1 Configuración Básica

Bajo la opción **Standard CMOS Setup** (puede tener otro nombre similar), se puede realizar la configuración básica de la BIOS, con la cual se puede ajustar la fecha y la hora del sistema, así como la configuración de discos duros y disqueteras. La pantalla de inicio para elegir esta opción suele ser similar a la mostrada en la siguiente figura.

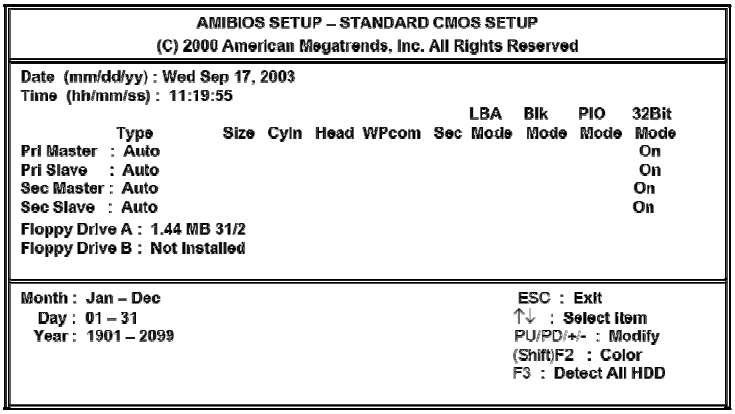


Figura 3.5 Standard CMOS Setup

Para cambiar la fecha y la hora debe situarse sobre ella e introducir la cifra actual, ya sea mediante el Mouse, las teclas correspondientes a los cursores o las teclas de avance y retroceso de página.

El tipo de disquetera y monitor es también común. En general la pantalla será VGA o bien EGA (este último no es frecuente); cuando dice “monocromo” suele referirse a pantallas MGA, ésas de fósforo blanco, verde o ámbar bastante antiguas, no a las VGA de escala de grises modernas.

Los discos durasen general son del tipo IDE (incluyendo los EIDE, Ata-4, Ultra-DMA y demás ampliaciones del estándar), en ningún caso SCSI no otros antiguos como MFM o ESDI, que se configuran de otras formas (mediante otra BIOS de la propia controladora SCSI). En las computadoras 486 y anteriores podremos dar valores sólo a dos discos duros, que se configuran como Maestro (Master) el primero y Esclavo (Slave) el segundo del único canal IDE disponible. En los controladores EIDE podremos configurar hasta cuatro, en dos canales IDE, cada uno con su maestro y su esclavo.

Los campos a completar suelen ser:

- **Tipo** (*Type)*: puede haber uno predefinido, o Auto para que calcule el µP los valores correctos, o User para introducir los valores a mano, o bien None para indicar que no hay ningún disco.
- **Tamaño** (*Size)*: lo calcula la computadora a partir de los datos que introducimos.
- **Cilindros** (*Cylindres)*: debe colocar la cantidad correcta.
- **Cabezas** (*Heads*): es otro dato (al igual que el anterior) que obtiene del manual del disco.
- **Precompensación de escritura** (*writePrecomp)*: es un parámetro muy técnico, usado sobre todo en los discos antiguos. Suele ser cero.
- **Zona de aparcado de las cabezas** (*LandZone*): es otro dato técnico, que suele ser cero o bien 65535.
- **Sectores** (*Sectores*): debe colocar la cantidad de sectores que hay en cada pista.
- **Modo de Funcionamiento** (*Mode*): para discos pequeños (de menos de 528MB) debe colocar Normal. Para discos de más de 528 MB, el modo LBA o bien Large, que debe colocar si no funciona el LBA. En muchos casos se permite la autodetección (opción Auto).

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.

3.5.2 Opciones de la BIOS

- **BIOS Feactures,** aquí se puede configurar, habilitar y deshabilitar determinadas prestaciones como la memoria caché interna y externa del µP, o fijar la opción de dónde irá a buscar el sistema operativo durante el arranque.

- **CPU Internal Cache**: habilita la caché interna del microprocesador. Debe habilitarse (poner Enabled) para cualquier chip con caché. Si la deshabilitamos, estaremos desaprovechando al µP pues bajará su rendimiento.

- **External Cache**: habilita la caché externa (de segundo nivel). No tiene tanta trascendencia como la interna, pero influye bastante en el rendimiento.

- **Quick Power On Self Test**: con esto podemos hacer que el test de comprobación al arrancar se haga más rápido.

- **Boot Sequence**: aquí se consigue que la CPU busque primero el sistema operativo en un disquete y luego en el disco duro si colocamos “A, C” o al revés si ponemos “C, A”. En BIOS actuales podemos hacer que la PC arranque desde una unidad ZIP o un CD-ROM.

- **Swap Floppy Drive:** si tenemos dos disqueteras (A y B), las intercambia el orden temporalmente.

- **Boot Up NumLock Status**: se usa para que el teclado numérico arranque configurado como cursores en vez de como números.

- **IDE HDD Block Mode:** un tipo de transferencia “por bloques” de la información del disco duro. Casi todos los discos duros de 100MB en adelante lo soportan.

- **Gate A20 Option**: en realidad no sé bien a qué hace referencia, pero corresponde a un dato técnico. Conviene colocar “conectado”.

- **Above 1 MB Memory Test:** aquí elegimos que verifique sólo el primer MB de RAM o toda (above = “por encima de”). Lo primero es más rápido pero menos seguro.

- **Memory Parity Check:** verifica el bit de paridad de la memoria RAM. Sólo debe usarse si la RAM posee esta opción, lo que no es usual, tanto en FPM como EDO o SDRAM.

- **Typematic Rate:** permite fijar el número de caracteres por segundo que aparece cuando pulsamos una tecla durante unos instantes sin soltarla.

- **Numeric Processor:** indica al ordenador que existe un coprocesador matemático. Esto ya no es útil pero si recibe una máquina vieja es interesante tenerlo en cuenta.

- **Security Option:** permite elegir si queremos usar una contraseña o **password** cada vez que arranquemos el equipo (System), sólo para modificar la BIOS (Setup o BIOS) o bien nunca (Disabled).

- **IDE Second Channel Option:** indica si vamos a usar o no el segundo canal IDE (sólo con controladores EIDE, claro), en cuyo caso le reserva una IRQ, generalmente la 15.

- **PCI/VGA Palette Snoop:** se suele utilizar cuando tenemos dos tarjetas de video o una de captura y los colores no aparecen correctamente. Es algo complejo y debe remitirse a la placa de video para mayor seguridad.

- **Video BIOS ROM Shadow:** si se habilita, copiará la BIOS de la tarjeta gráfica desde la ROM en la que está, a la rápida RAM del sistema, lo que acelera el rendimiento.

3.5.3 Configuración Avanzada y del Chisep

En esta opción podemos elegir distintos parámetros que indican qué características del chipset deben habilitarse y cómo se los habilitan. Afectan habitualmente a la memoria RAM, a las memorias cachés (internas y externas), a los buses ISA, VESA, PCI y AGP y otros dispositivos como los puertos serie y paralelo así como también al µP. Es quizá la parte más peligrosa, pues una equivocación puede inutilizar el sistema. Como primera recomendación, deje todo lo que pueda en Auto, aunque sacrifique algo de rendimiento.

Nota: aclaramos una vez más que los datos que presentó están basados en máquinas antiguas, que son las que más precisan de la atención del técnico o ingeniero, pero todo lo explicado es válido para computadoras provistas con Pentium III o 4, con chipset i815E, placas madres actuales, etc. Por supuesto que para mayor información refiérase al manual de su Placa Madre a la sección correspondiente al BIOS.

- **Auto Configuration:** aquí realiza una configuración automática. Los valores que aparecen en los demás ítems tras una primera autoconfiguración pueden ser válidos como punto de partida de un buen mantenimiento, así que apúntelos antes de modificarlos.

- **ISA Bus Clock**: ajusta la velocidad del bus ISA, que puede ser de unos 8 MHz. Se puede escribir como una cifra en MHz o en función del bus del sistema (el PCLK), por ejemplo, como 1/3 cuando éste es a 33 MHz, como en los 386 y 486 a 66 y 100. Cuando más rápido sea el bus, mejor (12 MHz es algo lógico), si coloca demasiado hasta puede hacer que las placas no funcionen.

- **Velocidad de la RAM**: cuanta mayor velocidad de la RAM indiquemos, más rápido irá el sistema, pero si la RAM no es tan rápida la estabilidad del sistema se resiente. Los valores que indican esta velocidad son los ciclos de acceso a RAM, los ciclos de espera (Clock Cycles o, a veces, Wait Status) del microprocesador a la RAM antes de escribir o leer de ella la información. En general existen opciones para configurar automáticamente estos valores; en algunas BIOS basta con introducir la velocidad en nanosegundos de la memoria, así como su tipo (normal –FPM-, EDO o SDRAM); en otras se debe poner la cifra más baja en ciclos. Por ejemplo, una ráfaga habitual en lectura (Read) puede ser 7-3-3-3, y se suele solicitar ese 3 como valor de DRAM Read Timing o DRAM Read Wait State (o Write para escritura). Para memorias EDO o FPM no tan viejas ese 3 puede ser un 2 y para SDRAM suele ser un 1. El 7 puede ser menor, incluso un 5 si tenemos un buen chipset y memoria rápida. Muchas veces se indica la velocidad de la memoria escribiendo Slower, Master y Fastest (de menos rápida a más rápida). Sugiero que coloque los valores por defecto y vaya subiéndolos (o bajándolos, si son ciclos de espera) de uno en uno, tras lo cual reinicie la computadora y observe el rendimiento y la estabilidad del procesador. En cuanto note inestabilidad, vuelva al valor anterior.

- **Ajustes de la caché:** el proceso es similar al explicado para la RAM. En algunas BIOS debe modificar los tiempos de acceso, en otros tendrá que modificar la forma de acceder a la caché. El modo Write Back es mejor que el Write Thru (o Through), aunque no puede usarse siempre, por eso le sugiero que sólo use esta opción cuando ya tenga experiencia.

- **Video y System Cacheable (Shadow):** aquí puede copiar la BIOS de la tarjeta de video o del sistema de la ROM a la RAM. Debería aumentar el rendimiento, pero puede dar problemas con sistemas operativos de 32 bits.

- **Manejo de dispositivos:** Los chipsets deben manejar las controladoras de dispositivos tales como discos duros, puertos serie, etc., que suelen estar incorporadas a la placa base. Por eso, deje esta opción por defecto.

- **Configuración por software de la CPU:** Muchas placas madre han dejado de lado el método clásico para configurar la CPU y emplean "puentes", autodetectando los valores correctos de velocidad de bus, multiplicador y voltaje y/o permitiendo que el usuario los seleccione mediante un sencillo menú en la BIOS. Hay programas como el SoftMenu que viene con las placas madre Abit (la BH6 por ejemplo), que realizan esta operación automáticamente.

3.5.4 Periféricos Integrados

Como vimos, las placas madre no tan antiguas (posteriores a las 486) suelen tener integrados los chips controladores del disco duro, y en muchas ocasiones manejan también las disqueteras, los puertos serie y paralelo. Por ello, las BIOS tienen diversos apartados para manejar estos dispositivos, entre ellos:

- **Conexión o desconexión de dichos controladores:** sirve para el caso del segundo canal IDE, que en ocasiones está deshabilitado por defecto, y que deberemos habilitar para conectar más de dos dispositivos IDE (o bien uno lento y uno rápido sin mezclarlos en el mismo canal, lo que baja el rendimiento).

- **Modos de acceso a discos duros (PIO y/o UltraDMA)**: generalmente puede elegir entre 5 modos PIO, del más lento, el PIO-0 hasta el más rápido, el modo PIO-4. También está el modo UltraDMA, aún más rápido. Si la controladora está integrada en la placa madre, debe especificar esos datos. Puede obtener estos datos del manual del disco duro, o en Internet en la página del fabricante o bien seleccione la opción Auto.

- **Direcciones e Interrupciones (IRQs) de los puertos**: debe saber si son los puertos serie o el paralelo. Generalmente debe seleccionar la configuración por defecto, pero si hay conflictos con otros dispositivos que usen esos mismos valores, deberán cambiarlo manualmente.

- **Tipo de puerto paralelo:** se suele poder seleccionar posibilidades como ECP o EPP. Debe buscar en el manual del periférico a controlar (un ZIP por ejemplo) para saber qué modo debe escoger.

- **Control del puerto de infrarrojos:** casi todas las placas madre traen los conectores para instalar un puerto de infrarrojos en su sistema. Generalmente deberán habilitarse y seleccionar su tipo, dirección de memoria, IRQ y si debe redireccionar la información de COM2 a este puerto (obviamente estos datos los brinda el fabricante del puerto infrarrojo).

3.5.5 Administración de Energía

En este menú se configuran las características de ahorro de energía de la computadora.

- **Power Management:** configura la administración de energía. Podemos habilitar el ahorro de energía, generalmente se ofrecen las opciones Disable (deshabilitado), User define (Definido por el usuario) y opciones predeterminadas para un ahorro mínimo o máximo.

- **PM Control by APM:** determina si el control de energía deberá hacerse según el estándar APM (Advanced Power Mangement, administrador avanzada de energía), lo que permite que Windows sea capaz de suspender el equipo a voluntad o, si utilizamos una fuente ATX, que el sistema se apague al pulsar “Apagar el Sistema” en el menú Inicio.

- **PM Timers:** permite controlar el tiempo que debe permanecer inactivo el sistema (System) o el disco duro (HDD) antes de que se active el ahorro de energía. Existen 3 grados de ahorro de energía:

    1. **Doze:** reduce la velocidad de la CPU (el microprocesador).
    2. **Standby:** reduce la actividad de toda la computadora.
    3. **Suspend:** reduce al mínimo la actividad del ordenador por lo cual se debe utilizar con CPUs tipo SL, como son la mayoría de los micro modernos.

- **PM Events:** configura una serie de ítems o sucesos que deben ser controlados para saber si el µP está inactivo o trabajando.

- **CPU Fan Off in Suspend**: si el ventilador de la CPU va conectado a la placa base, lo apaga cuando el equipo está en suspenso, ya que en ese momento la CPU está prácticamente parada.

- **Modem Wake Up:** activa el equipo cuando se detecta una llamada entrante en el Modem. El Modem debe estar conectado a la placa madre mediante un cable especial.

- **LAN Wake Up:** igual que la anterior, pero para la tarjeta de red. También necesita estar conectado a la placa madre.

3.5.6 Configuración de Plug & Play (PNP) y Slots PCI

Plug &Play, PNP o P&P: es una tecnología que facilita la conexión de dispositivos (es suficiente con conectarlo, el resto lo hace la computadora). No todos los dispositivos son PNP ni es una tecnología perfecta.

Aquí configura, entre otras cosas, las opciones de Plug & Play, por lo cual recomiendo colocar el ítem Auto, cada vez que sea posible, excepto que tenga inconveniente de IRQ entre dispositivos. La mayoría de dispositivos PCI soportan PNP, a diferencia de las tarjetas ISA, por eso, si la placa madre es antigua y no tiene slots PCI seguramente este menú no aparece. Las opciones son las siguientes:

- **PNP OS Installed:** informa al sistema si hay un sistema operativo PNP instalado, para que automáticamente se active el control de los dispositivos PNP. Lo que esta opción indique no afecta al correcto funcionamiento del sistema.

- **Resources Controlled by:** selecciona si los recursos controlados serán manuales o automáticos.

- **IRQx/DMAx assigned to:** selecciona una lista de las interrupciones (IRQs) y canales DMA que podemos asignar manualmente, para tarjetas **PCI/ISA PNP** o tarjetas **Legacy ISA** (tarjetas ISA no PNP, que son conflictivas). Es preciso conocer los valores de IRQ y/o DMA que se tiene que guardar y que obtiene del manual del dispositivo que trae conflicto.

- **PCI IDE IRQ Map to:** afecta a controladores IDE no integrados en la placa madre que no sean PNP.

- **Assign IRQ to USB:** aquí se selecciona si el puerto USB debe tener una interrupción asignada o no. Si no tiene ningún dispositivo USB conectado puede liberar esa IRQ para otros usos; suele se la misma interrupción que para uno de los slots PCI o ISA.

3.5.7 Autoconfiguración de la BIOS

En este menú encontrará varias funciones que facilitan la configuración de la BIOS dado que se realizan la selección de parámetros en forma automática.
Si bien tanto el tema de la BIOS como la explicación de Chipsets la hemos orientado a versiones antiguas de computadoras (por ser las que pueden llegar a nuestro taller para ser reparadas o actualizadas), todo lo dado se aplica a las computadoras de 2002, haciendo la aclaración que cada vez son las opciones que permiten la “autocorrección” de problemas y configuraciones automáticas. Por ejemplo, en el menú de autoconfiguración de la BIOS Ud. Puede encontrar las siguientes opciones:

- **Load BIOS Defaults:** determina una serie de valores automáticamente con poca optimización, generalmente útiles para volver a una posición de partida segura y resolver problemas observados al arrancar la computadora.

- **Load SYSTEM Defaults:** esta opción es dependiente de la BIOS. Generalmente asigna valores seguros (como LOAD BIOS DEFAULTS), pero en ocasiones carga valores optimizados para mejorar el rendimiento.

- **Load TURBO Defaults**: carga los valores óptimos para incrementar el rendimiento.

Además de las opciones vistas con relación a la BIOS, cabe aclarar que también podemos acceder a otras utilidades, tales como:

- **Autodetección de discos duros IDE:**Esta opción permite detectar los discos duros que están conectados al sistema y su configuración. Esto simplifica la tarea al instalar un disco nuevo. Una vez dentro de este menú, se detecta cada uno de los cuatro posibles dispositivos IDE. Apunte las opciones que le aparezcan y pruebe a usarlas; recuerde usar el modo LBA(excepto que tenga un disco muy antiguo de menos de 528 MB).

- **Control de Password:** Permite configurar una clave de acceso, pero si la olvida es posible que tenga que borrar la BIOS para volver a usar la computadora. Se puede generar esta clave ya sea en un menú específico o en las BIOS Feactures, seleccionando si quiero que la clave deba introducirla cada vez que arranca la PC o sólo si quiero ingresar en la BIOS.

- **HDD Low Level Format:** (Formateo de disco duro de bajo nivel). Genera un formateo más riguroso que el normal; ya que no sólo elimina los datos, sino que organiza la propia estructura del disco. Sólo se usa cuando el disco falla seguido o ha sido infectado por un virus resistente.

- **Antivirus:** Esta opción (que en ocasiones tiene un menú propio y en otras se engloba bajo un Standard Setup, con el nombre de Virus Warning) impide se escriba sobre la tabla de particiones o el sector de arranque del disco duro, pero no reemplaza a los programas antivirus. Con esto se busca impedir que un virus dañe el disco duro sin darle oportunidad a cargar un disquete de arranque con un antivirus para desinfectar el sistema; es decir, no impedirá la infección, pero es una medida más de seguridad. Por cierto, puede ser necesario deshabilitar esta opción durante la instalación del sistema operativo o al formatear el disco duro para que la BIOS no crea que se trate de un virus.

3.5.8 Cómo Salir del BIOS

Existen dos opciones:

- **Save and Exit Setup** (también puede ser **Write to CMOS and Exit**): aquí se graban los cambios antes de salir, con lo cual se reinicia el equipo. Debería pedirle confirmación, en forma de “Yes/No?”.
- **Exit Without Saving o Do not write to CMOS and Exit o Discard Changes and Exit:** salir sin guardar los cambios. También deberá indicar la confirmación.

3.6 Qué hacer cuando perdemos el password de la BIOS

Lamentablemente debe **borrar la BIOS entera.** Para ello existen tres formas:

1. **Por Software:** algunos programas se especializan en borrar BIOS, hay muchos dando vuelta por Internet (es un método que no recomiendo por ser peligroso).
2. **Por medio de un conector en la placa madre:** en algunas placas madres existe un jumper que al cerrarse y tras unos minutos de espera, permite borrar la BIOS sin inconvenientes posteriores.
3. **Desconectando la pila:** es un método poco ortodoxo pero efectivo.

Hay mucho para hablar sobre la BIOS pero creo que con este informe tiene un panorama amplio sobre la función de esta memoria.

3.7 Los Mensajes de Error del BIOS

Si al ejecutarse el POST se detecta algún error, el programa se detiene y emite un código de error en pantalla o un mensaje acústico, para indicarnos cuál es el problema encontrado. Sin embargo no se muestra el significado del código de error detectado.

Cuando aparece un mensaje de error, sea cual fuera, antes de efectuar cualquier reemplazo de partes debemos realizar todas las revisiones y pruebas necesarias para estar seguros de que dicho componente está defectuoso y se lo debe cambiar por otro. Cuando se detecta un error antes que estén preparados los mecanismos que permitan que dicha información se muestre en pantalla, el POST emite una señal de audio cuyas características indican el problema ocurrido. Estas señales dependen del fabricante y de la versión de la BIOS (no existe un estándar universal), sin embargo, casi todos responden a los estándares de AMI y Phoenix (Award).

Ahora bien, si por algún motivo no está seguro del sonido que escuchó (cuantos bips se emitieron, si fueron cortos o largos, etc.), reinicie el equipo y escúchelos para identificarlos en la tabla provista por el fabricante.

En la siguiente tabla se resumen los mensajes de error acústicos estandarizados por AMI.

Señal	**Error**
No hay ningún tono	La fuente de alimentación está mal o la placa madre está defectuosa.
Tono continuo	La motherboard está defectuosa.
Tonos cortos repetitivos	La motherboard está defectuosa.
2 tonos cortos y 1 largo	El monitor no esta conectado a la tarjeta de video.
3 tonos cortos y 1 largo	La tarjeta de video está defectuosa.
1 tono largo	Problemas en la memoria RAM o en la tarjeta de video.
1 tono largo y 1 corto	Falla en la placa madre.
1 tono largo y 2 cortos	Problemas en la tarjeta de video o en la configuración de XT.
1 tono largo y 3 cortos	Falla en la tarjeta EGA.
2 tonos largos y 1 corto	Falla en la información enviada al monitor.
1 tono corto con la pantalla en blanco	Problemas en el adaptador de video o en el cable del monitor.
1 tono corto	Problemas en el adaptador de video o en el cable del monitor.
2 tonos cortos	Se emite cuando hat error de paridad de memoria.

3 tonos cortos	La falla se encuentra en los primeros 64 KB de memoria RAM.
4 tonos cortos	Problemas en el temporizador.
5 tonos cortos	Problemas en el microprocesador o en la memoria de video.
6 tonos cortos	Problemas en la transferencia de información hacia el teclado.
7 tonos cortos	Problemas en el procesador virtual 8086.
8 tonos cortos	Falla la lectura y/o escritura en la memoria de video.
9 tonos cortos	Problemas en la BIOS.
10 tonos cortos	Error de lectura y/o escritura en el registro de apagado del CMOS.
11 tonos cortos	Problemas en la memoria caché externa.

En la tabla de abajo se brindan los mensajes de error acústicos para BIOS Award (Phoenix). Las señales emitidas no son tan claras como las producidas por una BIOS AMI, razón por la cual se debe prestar mucha atención.

Los mensajes se producen en una secuencia de tres grupos de tonos separados por dos pausas. Cada grupo está compuesto por una cantidad definida de tonos cortos (bips). En la tabla representamos la pausa con un asterisco y la cantidad de bips con números, por ejemplo, la indicación 1*2*3 significa un tono corto, una pausa, dos bips, otra pausa y 3 bips más. Excepto las tres primeras entradas de la Tabla que son códigos especiales y no cumplen con el estándar, el resto se identificarán de dicha manera.

Señal	**Error**
1*1*3	Falla de lectura y/o escritura del CMOS.
1*1*4	Error en la verificación de la BIOS.
1*2*1	Falla ubicada en el cronómetro de intervalos programables.
1*2*2	La falla se encuentra en la inicialización del DMA.
1*2*3	Falla en la E/S del registro de página del DMA.
1*3*1	Falla ubicada en la verificación del refresco de la memoria DRAM.
1*3*3	Falla en los primeros 64KB de RAM o en la línea de datos multibit.
1*3*4	Falla en la lógica par o impar de los primeros 64KB de RAM.
1*4*1	Falla en la línea de direcciones de los primeros 64KB de RAM.
1*4*2	Falla de paridad en los primeros 64KB de RAM.
1*4*3	Falla del reloj (EISA)
1*4*4	Falla en el puerto de software NMI (EISSA).
2*X*X	Falla en los primeros 64KB de RAM. Las dos X son bips que van del 1 al 4 y que nos identifican al bit defectuoso, del 0 al 15.
3*1*1	Problemas con el registro DMA maestro.
3*1*2	Falla en el registro DMA maestro.
3*1*3	Falla en el registro de máscara de interrupción maestro.
3*1*4	Falla en el registro de máscara de interrupción esclavo.
3*2*4	Falla en la verificación del controlador del teclado.
3*3*4	Problemas de comunicación con el monitor.
3*4*1	Falla en el trazado de la imagen.
3*4*2	No se encontró la ROM de video.
4*2*1	Falla en la verificación del cronómetro.
4*2*2	Falla en la prueba de reinicialización.
4*2*3	Falla en la línea A20.
4*2*4	Ocurrió una interrupción inesperada en el modo protegido.
4*3*1	Falla de direccionamiento durante la verificación de la memoria RAM.
4*3*2	Falla en el segundo canal del cronómetro programable.

4*3*3 Falla ubicada en el segundo canal del cronómetro.
4*3*4 Falla ubicada en el reloj de tiempo real.
4*4*1 Falla ubicada en el puerto serie.
4*4*2 Falla ubicada en el puerto paralelo.
4*4*3 Falla ubicada en el coprocesador matemático

También pueden darse los siguientes errores:

2 tonos cortos: Error de configuración del CMOS Setup.
1 tono largo y uno corto: Falla en la placa de video.
1 tono largo, uno corto, otro largo y otro corto: Falla en la placa de video.

Por último, damos a continuación una serie de códigos de error que pueden aparecer en pantalla cuando el POST no se ha ejecutado correctamente. Cabe aclarar que no es complejo "descifrar" la estructura de estos códigos, pero su estudio no es objeto de esta obra.

Código	Error	Código	Error
01X	Error indefinido	134	Error en la lógica del arbitraje del DMA
02X	Falla en la fuente de alimentación	151	Falla en la memoria RAM del CMOS; en el tiempo real
1XX	Motherboard	152	Falla en la memoria RAM del CMOS
101	Falla por interrupción	161	Falla en la batería del CMOS
102	Falla en el temporizador	162	Configuración errónea del CMOS
103	Falla en una línea de interrupción	163	Fecha y hora erróneas en el CMOS
104	Falla en el modo protegido	164	Tamaño de memoria en CMOS incorrecto
105	El último comando 8042 no fue aceptado, problemas con el controlador del teclado.	165	PS/2 desconoce la configuración de una tarjeta
106	Falla en la conversión lógica	166	Tiempo de respuesta de un adaptador sobrepasado PS/2
107	Falla en el coprocesador matemático	167	El reloj del sistema no está actualizado PS/2
108	Falla en el temporizador del bus	168	Error en la configuración del CMOS del coprocesador matemático
109	Falla en el DMA	169	Configuración incorrecta en la motherboard
110	Error de paridad (PS/2)	170	Conflicto en la configuración ASCII
111	Falla en la memoria de expansión	171	Fallas en el diagnóstico del CMOS
112	Error de arbitraje el bus MCA	172	Falla en el diagnóstico de la NVRAM.
113	Error de arbitraje en el DMA del bus MCA (PS/2)	173	Suma de verificación incorrecta en el CMOS / NVRAM
114	Error de verificación en la ROM externa	174	Configuración del sistema incorrecto
115	Error de paridad en la memoria caché; error de verificación de la ROM del BIOS; error en DMA o CPU defectuosa.	175	CRC incorrecto en la EEPROM
116	Error de E/S en un puerto	177	CRC de la contraseña ingresada incorrecto.
118	Error en la memoria caché externa	178	EEPROM defectuosa
119	Unidad de disquete de 2.88 MB instalada, pero no soportada por el controlador de unidades de disco.	179	Log de errores de la NVRAM completo
120	Error en la memoria caché interna	180X	Error de datos en el slot X
121	Interrupciones inesperadas.	181	Configuración no soportada
133	Error en la verificación lógica del DMA	183	El sistema esta bloqueado, se requiere la contraseña correcta
184	Contraseña de encendido incorrecta	306	Teclado incorrecto; el BIOS no soporta el teclado conectado
185	Secuencia de inicialización incorrecta	341	Error en el teclado
186	Falla en el hardware de protección por contraseña.	342	Error en el cable del teclado
187	Número de serie incorrecto	343	Error en la tarjeta mejorada o en el cable del teclado
188	Suma de verificación de la EEPROM incorrecta.	365	Falla en el teclado
189	Se superó el límite de intentos con contraseñas incorrecto.	366	Falla en el cable de la interfaz del teclado
191	Falla en la prueba del controlador de	367	Ídem 343

	memoria caché 82385.		
194	La memoria presenta fallas	4XX	Tarjeta de video monocromática (MDA)
199	Error en la configuración	401	Falla en la prueba de frecuencia de sincronismo horizontal del adaptador, error en la memoria del adaptador
2XX	Memoria RAM	408	Falla en los atributos de los caracteres
201	Falla en la prueba de memoria	416	Falla en el juego de caracteres utilizado
202	Error en la dirección de memoria dada: A0-A15	424	No se puede activar el modo texto 80x25
203	Error en la dirección de memoria dada: A16-A23	432	Falla en la prueba del puerto paralelo de tarjeta monocromática
215	Falla en la memoria (PS/2)	5XX	Tarjeta CGA
221	Falló la copia de la ROM a RAM (Shadow RAM) para MCA	508	Falla en los atributos de los caracteres
225	La memoria conectada es de velocidad incorrecta para MCA	516	Falla en el juego de caracteres utilizado
231	La memoria instalada vía tarjeta adaptadora no es contigua	6XX	Unidad de disquete / controlador
241	Fallas en el tercer módulo de la memoria	601	Falla en el autotesteo de la unidad o controlador
3XX	Problemas de teclado	602	Registro de arranque del disquete no válido
301	Error en el teclado	603	Tamaño del disquete no válido
302	El teclado se encuentra bloqueado	604	Error en la detección del medio
303	Teclado defectuoso, el controlador del teclado no responde	605	Unidad de disquete bloqueada
304	Falla al tratar de controlar el teclado; el reloj del teclado está trabajando a frecuencias mas altas de las normales	606	Falla en la función de verificación de cambio de diskette
305	Faltan los +5V en los conectores PS/2	607	Disquete protegido contra escritura
608	Error en el estado de los disquetes	656	Falla en el mecanismo de la unidad
610	Falla en el formato del disquete	7XX	Coprocesador matemático
611	La unidad no reacciona, tiempo terminado	702	Falló la prueba del coprocesador
612	Chip o controlador de disquete defectuoso	707	Falla en la prueba de unión
613/614	El adaptador falló en la prueba de DMA	708	Falla en la prueba de carga y almacenamiento de enteros
616	Número de revoluciones incorrecto error de velocidad del motor	711	Error al guardar estados
621	Error de posicionamiento / búsqueda	712	Falla en la prueba de modo protegido
622	Se encontró CRC defectuoso	713	Falla en la prueba de sensibilidad a tensión de operación y temperatura
623	No se encontró el sector	9XX	Primer puerto paralelo (LPT1)
624	Marca de dirección incorrecta	901	Error en el autotesteo de los puertos
625	Error de posicionamiento / búsqueda, falla en controlador	902	Error en el registro de control
626	Error en comparación de datos del disquete	903	Error en el registro de decodificación de direcciones
627	Error en la línea de cambio de disquete	904	Error en la decodificación de direcciones
628	El disco se retiro de la unidad en forma prematura	910	Error en la conexión (línea de estado).
645	No hay pulso índice	911	Error en el bit 8 de la línea de estado
646	Ha fallado la detección de la pista 0 de la unidad	912	Error en el bit 7 de la línea de estado
648	La prueba de formato ha fallado	913	Error en el bit 6 de la línea de estado
649	Se encontró un medio incorrecto en la unidad	914	Error en el bit 5 de la línea de estado
650	Ídem 616	915	Error en el bit 4 de la línea de estado
651	Falla en el formato	916	Se producen interrupciones incorrectas
652	Falla de verificación	917	Se produjo una interrupción inesperada en el adaptador de la impresora
653	Falla de lectura	92X	Error en el registro X
654	Falla de escritura	1106	No se puede apagar la opción serie
655	Error en el controlador de la unidad	1107	Error en la interfaz
1108	Error durante la IRQ 3	1135	No hay interrupciones
1109	Error durante la IRQ 4	1136	No se produjo la interrupción de línea recibida.
1110	Falla en un registro (16450/16550)	1137	No hay datos disponibles para recibir

1111	Error en la prueba de la línea de control del UART
1112	Ídem 1111
1113	Error de transmisión del UART
1114	Error de recepción del UART
1116	Error en la interrupción del UART
1117	Falla en velocidad de transmisión
1118	Error en la recepción de datos manejada por interrupciones del UART
1119	Falla en el buffer FIFO del UART
1120	Falla al asignar valores al registro de habilitación de interrupciones del UART
1121	Ídem 1120
1122	Error de interrupción pendiente
1123	Error en el registro de identificación de interrupciones
1124	Falla al asignar valores al registro de control del módem
1126	Falla al asignar valores al registro de estado del módem
1128	Error en la identificación de una interrupción
1129	No se pudo forzar otra ejecución
1130	No se produjo la interrupción del estado del módem
1131	La interrupción pendiente no válida
1132	No hay señal DR
1133	No hay datos disponibles luego de una interrupción
1134	No se espera por una transmisión luego de una interrupción
1138	El registro de transmisión en espera no está vacío
1139	Ídem 1130
1140	Ídem 1138
1141	Ídem 1135
1145	Error en la velocidad de transferencia máxima
1146	Error en la velocidad de transferencia mínima
1148	El tiempo de respuesta expiró
1149	Datos retornados no válidos
1150	Error en el registro del estado del módem
13XX	Puerto de juegos (GAME PORT)
1301	Error en el autotesteo de los puertos
1302	Falla en la prueba del joystick
14XX	Impresora
1401	Error en el autotesteo de la impresora
1402	Falla en la prueba de la impresora
1403	La impresora se quedó sin papel
1404	Falla en la prueba de la impresora
1405	Falla en el adaptador del puerto paralelo
1406	Falla en la prueba de la impresora
15XX	Adaptador SDLC
1510	Falla en el puerto B 8255
1511	Falla en el puerto A 8255
1513	El timer 8253 no alcanzó la cuenta final
1514	Timer 8253 1 atorado
1515	El timer 8253 0 no alcanzó la cuenta final
1516	Timer 8253 0 atorado
1517	El timer 8253 2 no alcanzó la cuenta final
1518	Timer 8253 2 atorado
1519	Error en el puerto B de 8273
1520	Error en el puerto A de 8273
1522	Falla de la línea de interrupción nivel 4

CAPÍTULO 4
LAS AMENAZAS DE LOS SISTEMA INFORMÁTICOS

4.1 Los Virus Informáticos

4.1.1 Introducción

Virus. Todo el mundo ha oído hablar de ellos y muchos han sufrido por su culpa, pero su forma de infectar, reproducirse o atacar sigue siendo un gran misterio para la mayoría. Una antigua máxima reza: "Si quieres vencer a tu enemigo, conócelo primero". Eso es lo que se intentará: si se ejecutan en un ordenador, es que son programas. Y si son programas, se pueden comprender. Es cierto que no contamos con el código fuente, pero ¿acaso es imprescindible? ¿Es que no tenemos el código objeto...?

Desde que en 1987 se diera el primer caso documentado de ataque de un virus informático en la Universidad de Delaware, mucho se ha dicho y escrito sobre el tema dentro de los foros más insospechados. A pesar de ello los virus siguen siendo grandes desconocidos para la gran mayoría, razón que sin duda contribuye no poco a que cada vez sea mayor el número de ellos en expansión. Conocer y entender la forma en que actúan, se reproducen y se comportan es la mejor forma de estar prevenido y saber cómo reaccionar; la solución de formatear el disco duro nada más enterarse de que dentro hay un virus es bastante extrema y, por lo demás, suele eliminar toda la información del disco duro... a excepción del propio virus.

Por otra parte, ya no en el caso de un particular, sino en el de las empresas, es muy posible que no puedan permitirse esperar a que se saque la siguiente versión de un antivirus que elimine el que les afecta, y necesiten que alguien realice un estudio inmediato de su virus, identifique su forma de actuar, sus efectos, y se pueda poner a corregirlos cuanto antes.

Esta serie de temas tratará de dar cumplida visión del funcionamiento y técnicas de estos programas, pensando que el conocimiento y el entendimiento son dos armas básicas en la lucha contra cualquier amenaza.

Hay quien opina que este tipo de información no debe hacerse pública para evitar que más gente se dedique a fabricar virus. Pero, ya que según los estudiosos la media de aparición de virus nuevos viene a ser de unos 5 o 6 cada día -por no contar las modificaciones y mutaciones sobre otros ya existentes-, es fácil llegar a la conclusión de que "los malos" ya tienen toda la información que necesitan. Normalmente las políticas de ocultación de información de este tipo con ánimo de evitar que se utilice con "malos fines" fracasan estrepitosamente al acabar siempre desinformados los que sufren los ataques y nunca quienes los perpetran, cosa que ayuda a que los ataques sean mucho más efectivos.

Por eso aquí se tratará con virus reales, estudiando su comportamiento a través de su propio código. La naturaleza de estos programas obliga, eso sí, a suponer en el lector tiene

conocimientos mínimos de lenguaje ensamblador. Se explicarán construcciones crípticas u operaciones poco evidentes por estar fuertemente ligadas a la arquitectura de la máquina, pero no el repertorio de instrucciones o los modos de direccionamiento.

4.1.2 Historia

La paternidad de la idea de un programa capaz de reproducirse se le atribuye a John von Neumann por su artículo "Theory and Organization of Complicated Automata" del año 1949. Von Neumann estaba interesado en la creación de vidas artificiales electrónicamente, a las que daba el nombre de autómatas que, según él, podían reproducirse sin excesiva dificultad.

También por aquel entonces, cuando empezaban a desarrollarse los primeros ordenadores, se vio la necesidad de llevar a la computadora a un estado inicial conocido, eliminando rastros de otros programas previamente cargados. Una solución muy ingeniosa consistía en implementar una instrucción que simplemente se copiaba a la siguiente posición de memoria y saltaba a ella para seguir ejecutándose. De esta forma todo el mapa de memoria se llenaba con un único valor conocido: el código correspondiente a la instrucción. Este fue otro ejemplo claro de código capaz de reproducirse. Seguramente basado en él, más adelante, en los años 60, cobró gran popularidad el juego "Core Wars", diseñado en los laboratorios Bell de AT&T: dos jugadores lanzaban simultáneamente sus programas que se reproducían en memoria hasta que ésta se agotaba. Ganaba aquel que fuera capaz de "conquistar" más memoria, para lo cual era perfectamente legal "matar" a las copias del adversario y "robarle" esa memoria.

Aparte del meramente lúdico, también se trató de darle un uso algo más práctico a este tipo de programas, y así, a finales de los años 70, dos investigadores del Centro de Investigación Xerox de Palo Alto, California, idearon un programa que debía encargarse de las labores de mantenimiento y administración del complejo, al que dieron el nombre de "gusano". El programa "dormía" por el día y por la noche se propagaba por todos los ordenadores del Centro haciendo copias de seguridad y otras tareas de gestión. Todo esto en la teoría, porque en la práctica el gusano escapó de los ordenadores de prueba del laboratorio, se extendió por toda la red y paralizó todas las máquinas. Al intentar eliminarlo, seguía reapareciendo, así que no hubo más remedio que crear otro programa vermicida que fuera por todas las máquinas matando copias del gusano.

- **Los años 80**

La palabra virus no se empezó a usar hasta que Fred Cohen, un estudiante graduado de la Universidad del Sur de California, lo utilizó en 1984 para su tesis sobre programas autoduplicadores. En ella daba la primera definición formal del término y hacía un estudio matemático de la expansión de este tipo de engendros, mediante el cual demostró que crear un programa detector de virus perfecto era lógicamente imposible.

Ningún detector de virus puede ser perfecto. En su tesis doctoral para la Universidad de California, Los Ángeles, Fred Cohen demostraba, en 1983, que no hay ningún algoritmo general que pueda concluir con total fiabilidad -100%- si un programa es o no un virus. Para ello se valía de la siguiente demostración por reducción al absurdo: Supóngase que existe un algoritmo general “A” que, analizando cualquier programa “P”, devuelve "true" si y sólo si “P”

es un virus. Entonces sería posible crear un programa, “P”, que hiciera lo siguiente: if (A(P) = false) then infecta el sistema if (A(P) = true) then no infectes nada Es decir: “P” es un virus si “A” dice que no lo es, y no lo es si “A” dice que lo es. Por contradicción, ese algoritmo general “A” no existe.

Como se dijo antes, en 1987, el 22 de octubre, se da el primer ataque de virus del que se tiene noticia. En realidad era inofensivo y contenía la dirección y teléfono de los autores: dos hermanos de Pakistán, estudiantes de la Universidad de Lahore, aunque, al parecer, hubo un estudiante que perdió su tesis debido a efectos secundarios del virus. También ese año se produce la primera infección masiva sobre ordenadores Macintosh: un consultor de Aldus Corporation se infectó con un disco de juegos y al realizar luego pruebas al programa Aldus Freehand contaminó el disco que luego distribuyó su empresa. El virus se limitaba a presentar en pantalla: "mensaje universal de paz" a todos los usuarios del Mac, firmado por Richard Brandow, editor de la revista MacMag, al llegar al 2 de Marzo de 1988 (fecha del aniversario de la aparición del Macintosh II) y se autodestruía inmediatamente. Pero los buenos deseos de paz pronto se transformaron en sentimientos menos encomiables. Así, tiempo después, un banco de la isla de Malta se vio afectado por un virus que sacaba el siguiente mensaje por pantalla:

"DISK DESTROYER - A SOUVENIR OF MALTA / I have just DESTROYED the FAT on your Disk!! / However, I have kept a copy in RAM, / and I'm giving you / a last chance to restore your precious data./ WARNING: IF YOU RESET NOW ALL YOUR / DATA / WILL BE LOST FOREVER!! / Your data depends on a game of JACKPOT / CASINO DE MALTE JACKPOT/ +L+ +?+ +C+ / CREDITS: 5 / < >"

El virus borraba la FAT, una estructura básica de cualquier disco DOS que permite encontrar los datos, pero guardaba una copia en memoria. Después invitaba a jugar a las tragaperras: si salían tres "L", restauraba la FAT y no se perdían datos, pero si salían tres "?" o tres "C", destruía también la copia de RAM y se perdían todos los datos. Como era de esperar, el banco perdió la información en dos terceras partes de sus máquinas.

- **Los primeros virus (1985-1987)**

En este año, 1986, Basit y Amjad se percataron de que el sector boot de un disquete contenía código ejecutable, y que este código corría siempre que se reiniciaba el PC con un disquete en A:. También se dieron cuenta de que podía reemplazar código con su propio programa, pudiendo ser éste un programa en la memoria residente, y que podía instalar una copia de sí mismo en cada disquete, accesible desde cualquier dispositivo. Como el programa se copiaba a sí mismo, le dieron el nombre de 'virus', por su semejanza con los virus biológicos. Este proyecto de virus solamente infectó 360Kb de disquetes. También en 1986, un programador llamado Ralf Burger vio que un archivo podía hacer una copia de sí mismo por el método simple de atacharla en otros archivos. Entonces desarrolló una demostración de este efecto, que llamó 'Virdem'. Lo distribuyó en la 'Chaos Computer Conference' de diciembre de ese año, en la cual el tema principal eran precisamente los virus. La demostración tuvo tanto éxito que Burger escribió un libro sobre el tema, en el que no se mencionaba aún a los virus del sector de arranque.

Al año siguiente, 1987, la Universidad de Delaware se dio cuenta de que tenía un virus cuando empezaron a ver una extraña y sospechosa 'etiqueta' que aparecía en los disquetes.

Y eso es todo lo que este pequeño virus hacía (autoreplicarse y colocar una 'etiqueta'). La alerta la dio una empleada de soporte técnico de la misma Universidad, que advirtió de que estaba encontrando la 'etiqueta' en muchos de los disquetes. Este mismo año, Franz Swoboda tuvo noticia de un virus incluido en un programa llamado 'Charlie'. Por ello, le llamó el 'Virus Charlie'. Hubo mucho revuelo en la opinión pública acerca de este virus, al difundirse las dos versiones de una misma historia: Burger afirmó que había obtenido una copia del virus de manos de Swoboda, pero Swoboda lo negó siempre. En cualquier caso, Burger se hizo con esa copia que envió a Bernt Fix, el cual 'desarmó' el virus, y Burger incluyó en su libro la demostración del análisis, después de añadirle varios parches para variar su comportamiento. El comportamiento normal de 'Vienna' (o 'Charlie', como lo llamaba Swoboda) era colocar un archivo entre otros ocho para reiniciar el PC (el virus 'parchea' los primeros cinco bytes de código); Burger (o quizá Fix) reemplazaron este código con cinco espacios. El efecto fue que los archivos 'parcheados' colgaban el PC, en vez de reiniciarlo. No era una mejora muy satisfactoria.

Mientras tanto, en los Estados Unidos Fred Cohen acababa de completar su tesis doctoral, que versaba precisamente sobre los virus informáticos. El doctor Cohen demostró que uno no puede escribir un programa que sea capaz de, con un cien por cien de aciertos, visualizar un archivo y decidir si es o no un virus. Desde luego, nadie pensó jamás en esa posibilidad, pero Cohen hizo buen uso de un teorema matemático, y así fue como se ganó el doctorado. Sus experimentos sobre la difusión de virus en los sistemas informáticos demostraron que la expansión de las infecciones resultaba ser mucho más rápida de lo que nadie hubiera esperado.

En 1987, Cohen visitó la Universidad Lehigh, y allí se encontró con Ken van Wyk. De este encuentro surgió el virus 'Lehigh', que nunca abandonó el laboratorio, porque sólo podía infectar COMMAND.COM y dañar increíblemente su host después de tan sólo cuatro replicaciones. Una de las reglas básicas sobre los virus es que aquel de ellos que dañe de forma muy rápida su host, no sobrevive durante mucho tiempo. De todas formas, el virus Lehigh se hizo muy popular, y fomentó la aparición del grupo de noticias sobre virus de Ken van Wyk en Usenet.

- **En 1988: Aparecen los Antivirus comerciales**

Este año será recordado siempre entre los expertos en seguridad informática. De hecho, fue el año en el que comenzaron a aparecer los fabricantes de anti-virus, creando una moda de lo que en principio sólo era un problema potencial. Los vendedores de software anti-virus eran pequeñas compañías, que ofrecían sus productos a muy bajo precio, en algunos casos gratuitamente. La compañía IBM se dio cuenta de que tenía que tomarse el asunto de los virus completamente en serio. Esta conclusión no la tomaron debido a la incidencia del popular 'gusano del árbol de Navidad', de amplia difusión, sino porque IBM sufrió un brote del virus 'Cascade', y se encontró en la embarazosa necesidad de tener que comunicar a sus clientes que ellos también habían sido infectados. Desde este momento, el 'High Integrity Laboratory' de IBM fue el encargado del área virus.

En 1988 aparecieron, desde luego, múltiples rebrotes de 'Brain', 'Italian', 'Stoned', 'Cascade' y 'Jerusalem'. Esto representó la prueba definitiva de la existencia real de los virus. Peter Norton, en una entrevista, había comentado que eran una leyenda urbana, como los cocodrilos de las alcantarillas de Nueva York, y un experto informático del Reino Unido llegó

a proclamar que tenía la prueba de que los virus eran un producto de la imaginación de mentes calenturientas...

En aquel momento, cada nueva aparición de virus provocaba la aplicación de un análisis paso-a-paso. El software existente era utilizado para detectar virus de sector de arranque, y solamente fue escrito un programa anti-virus, de manera excepcional, para afrontar los rebrotes de 'Cascade' y 'Jerusalem'. Entonces apareció el virus "B", el cual no se alojaba en memoria residente, y resultó ser una modificación de aquel que borraba los archivos todos los viernes y 13. Cuando 'Virus-B' se ponía en funcionamiento, desplegaba el siguiente mensaje:

"Warning! This program is infected with Virus-B! It will infect every .COM file in the current sub directory!".

Un virus que se manifiesta de una manera tan obvia, obviamente no puede ser tan pernicioso: evidentemente, se trata de la demostración de la forma de actuación de un virus, de ahí el mensaje.

A finales de 1988 se dieron varios sucesos importantes. En primer lugar, se produjo la aparatosa intrusión del virus 'Jerusalem' en una importante institución financiera, que durante varios días se vio en la necesidad de 'limpiar' a conciencia sus bases de datos. Por otro lado, la compañía S&S impartió el primer 'Seminario sobre Virus', en el cual se explicó pormenorizadamente lo que era un virus y de qué forma actuaba. Por último, en enero del año siguiente rebrotó otra vez 'Jerusalem', como todos los viernes y 13, y se difundió ampliamente en diversas empresas e instituciones... Estaba clara la necesidad de una herramienta que permitiera limpiar masivamente los sistemas de cualquier virus en activo. El doctor Alan Solomon, consciente de esta necesidad, desarrolló un anti-virus, le añadió algunas herramientas que, según su experiencia, podían ser útiles, y creó de esta forma la primera herramienta anti-virus, 'Dr. Solomon's Anti-Virus Toolkit'.

A finales de 1988, 'Jerusalem' se había difundido de forma espectacular por España y Reino Unido. Debido al comportamiento destructivo de este virus, los expertos llegaron a la conclusión de que era necesario habilitar algún tipo de alarma para alertar a los usuarios. Pero los medios de comunicación también entraron en el juego: la posibilidad de predecir la aparición de un virus cautivó su imaginación, y de esta forma la actividad de los virus informáticos traspasó las fronteras de las universidades y empresas de informática y llegó al usuario habitual de PC’s.

- **El año de la expansión (1989)**

1989 fue el año en el que las cosas se pusieron difíciles. El virus 'Fu Manchú' (una modificación del 'Jerusalem') fue difundido por alguien anónimo en el Reino Unido, junto con el '405'. Por otra parte, los búlgaros y los rusos empezaron a interesarse por el tema. En marzo de este año, un pequeño incidente fue el aviso de la gran avalancha que se avecinaba: en Holanda, un tal Fred Vogel contactó a Alan Solomom, para contarle que había encontrado un virus nuevo en su disco duro, llamado 'Datacrime', y que estaba preocupado porque al parecer, su fecha de activación estaba prevista para el día 13 del mes siguiente.

Cuando el virus fue analizado, sin embargo, se llegó a la conclusión de que, cualquier día después del 12 de octubre de 1989, podría formatear a bajo nivel el cilindro cero del disco duro, lo cual en la mayoría de los discos, borraría la FAT, dejando al usuario sin su información. También se desplegaba un mensaje con el nombre del virus, 'Datacrime'.

Se redactó un informe sobre los efectos de este virus, que se publicó en una revista, y otros medios de comunicación se hicieron eco del caso, llegando en Junio a la errónea conclusión de que este virus se activaría cada 12 de octubre, cuando en realidad podría activarse cualquier día entre el 12/10 y el 31/12 y era capaz de borrar toda la información contenida en el disco duro.

En Norteamérica, la prensa empezó a llamarle 'El virus del Descubrimiento', y se corrió la voz de que había sido escrito por terroristas noruegos, hartos de que se otorgara la autoría del Descubrimiento de América a Colón, en vez de a Erik el Rojo.

Mientras en Holanda la policía empezó a distribuir un detector del virus 'Datacrime', vendiéndolo a un dólar en todas las comisarías de policía. Se vendió muy bien, pero daba una serie de falsas alarmas, por lo que enseguida fue sustituido por una segunda versión. Esto provocó mucha confusión en la opinión pública, porque realmente nadie era capaz de saber si tenía o no el virus. En el mes de julio, debido al mayor índice de concientización ciudadana, un gran número de compañías holandesas solicitaron información a IBM sobre si los virus eran realmente un problema serio. Existían muchas posibilidades de que una empresa pudiera infectarse de 'Datacrime', 'Jerusalem', 'Cascade' o 'Stoned'. IBM contaba con un programa software de detección y eliminación de virus para su uso interno, que si no ofrecían inmediatamente a sus clientes, podía representar un menoscabo en su reputación. Los técnicos sabían que en cualquier momento podría producirse una infección masiva de cualquiera de estos virus, en especial de 'Datacrime'. En septiembre de 1989, IBM lanzó su versión 1.0 de este escáner, junto con una carta en la que explicaba a sus clientes lo que era y para qué servía. Las empresas usaron el software, y se encontraron con que no estaban infectados por 'Datacrime', pero sí por multitud de versiones de los virus vigentes en ese momento.

El 13 de octubre de ese año fue viernes, y por tanto fecha posible de activación de dos de los virus más conocidos en aquel momento: 'Jerusalem' y 'Datacrime'. En los Estados Unidos, los avisos de alerta sobre la actividad de 'Datacrime' habían sido excesivos, dado el carácter prácticamente inocuo del citado código, pero no se registró ninguna infección. En Europa, sólo afectó a unos pocos usuarios. El Instituto Nacional de Ciegos (RNIB) anunció que había sido infectado, y que había perdido gran cantidad de datos de sus cuentas y muchos meses de trabajo. Pero se trataba de una infección de baja intensidad de 'Jerusalem', que había borrado unos cuantos archivos fácilmente reemplazables. Cuatro PC's fueron infectados, pero este hecho pasó a la historia de los virus como "el Gran Desastre del RNIB".

Este año tan agitado terminó con la distribución de 20.000 copias de un famoso código malicioso, el Aids Information Disquette, que fueron enviadas por correo a usuarios que figuraban en bases de datos de diversos organismos, por ejemplo el PC Business World. Este documento contenía instrucciones de instalación detalladas que originaban la creación de archivos y directorios ocultos, editando el contenido de AUTOEXEC.BAT, de modo que

uno de estos archivos estaba presente en cada motor de arranque. El 'troyano' que contenía encriptaba todos los archivos del disco duro, otorgándoles los atributos alojados en él.

La consecuencia más destacada de este incidente es que consiguió otorgar mayor popularidad a los virus, aunque el código malicioso protagonista del hecho en realidad era un troyano. Además, un sorprendente número de personas instalaron el software, de tal manera que PC Business World tuvo que desarrollar un programa para solucionar los desaguisados que provocó la distribución de este 'troyano'.

- **1990: Se crea el primer virus polimórfico**

En el año 1990, surgieron algunas novedades en el panorama de los virus. Mark Washburn había creado el primer virus polimórfico a partir del 'Viena'. Los virus polimórficos representaron un paso adelante en la evolución de los códigos malignos, al ser capaces de encriptar de forma diferente su código cada vez que cometían una nueva infección; por ello, era necesario desarrollar un algoritmo que pudiera aplicar tests lógicos al archivo, decidiendo de esta manera si los bytes eran malignos o no, para crear la herramienta anti-virus que bloqueara dichos códigos.

Aunque Washburn publicó el código de su virus, y se temió que muchos creadores de virus decidieran crear nuevos códigos a partir de aquel, la invasión de virus polimórficos no tuvo lugar en el mercado. Además, la mayoría de las empresas del sector (excepto Virus Bulletin, IBM y pocos más) tampoco fueron capaces de desarrollar herramientas anti-virus apropiadas, ya que no es tan fácil crear un algoritmo de desencriptación. No obstante, la idea del polimorfismo se ha utilizado profusamente después en la creación de 'criaturas víricas' más modernas.

Otra de las consecuencias de los virus polimórficos es el incremento de las falsas alarmas. Si un vendedor de software anti-virus consigue escribir el software apropiado para detectar algo con tantas posibilidades de mutación como 'Viena', existen muchas posibilidades de que en realidad lo que el escáner detecte sea una línea de código inofensivo. Y una falsa alarma puede ser más engorrosa para el usuario que un auténtico virus, ya que obliga a poner en funcionamiento absolutamente todos los mecanismos anti-virus de defensa.

También en 1990 asistimos a una oleada de virus procedentes de Bulgaria, especialmente de aquellos cuyo autor se identificaba con el alias 'Dark Avenger'. Los virus 'Dark Avenger' introdujeron dos conceptos nuevos: la infección rápida (el virus se instalaba en la memoria, y la simple apertura de un archivo provocaba una infección vertiginosa del disco duro) y el ataque remoto (algunos de estos virus sobrescribían código cada cierto tiempo, por lo que si el usuario no se daba cuenta y hacía 'backup' de los datos periódicamente, autoreplicaba sin querer todas las líneas de código maligno). Otros virus clásicos de parecida actuación durante este periodo fueron 'Number-of-the-Beast' y 'Nomenklatura'.

Sin embargo, 'Dark Avenger' era el más creativo en el proceso de distribución de sus virus. Cargaba sus códigos malignos en BBS's, infectando los programas anti-virus shareware, y en sus ataques víricos incluía un archivo que cumplía la función de tranquilizar a todo aquel que comprobara el tamaño del archivo o realizara un 'checksumming'. Incluso

se permitía el lujo de incluir su código fuente para que los legos pudieran aprender cómo se creaban virus.

En este mismo año tuvo lugar otro evento en Bulgaria: la aparición de la primera BBS de intercambio de virus. En ella la gente podía descargarse cualquier virus en el que estuviera interesado, si previamente había dejado algún código maligno propio para los usuarios de este sistema. Esto, claro está, favoreció tanto la creación de nuevos virus como la difusión masiva de muchos de ellos.

- **1991: Lanzamiento de Antivirus y virus polimórficos**

En el año 1991, el problema de los virus ya era lo suficientemente preocupante como para atraer a las grandes compañías de marketing. Symantec lanzó a principios de este año el producto Norton Anti Virus, y Central Point CPAV en abril. Pronto los siguieron Xtree, Fifth Generation y unos cuantos más. Muchas de estas compañías reutilizaron los programas de otras empresas (casi todas israelíes). Pero el gran problema de este año fue el llamado 'glut'. En diciembre de 1990, había alrededor de 100 ó 300 virus. En diciembre del siguiente año, 1000 (ya que en este año se escribieron gran cantidad de virus). 'Glut' quiere decir algo así como 'superabundancia', lo cual, referido al tema de proliferación de virus, causó la aparición de múltiples y desagradables nuevos problemas. Los programas tenían muchas limitaciones. En particular, era necesario el almacenamiento de gran cantidad de datos en memoria para proceder a un escaneo en busca de virus, y bajo DOS sólo había disponibles 640 Kb utilizables. Otro problema es que algunos escáneres eran demasiado lentos, en proporción al gran número de virus que debían detectar. Además, el análisis de virus requiere no sólo su detección real, sino su desinfección efectiva. Si cada día hubiera que proceder al análisis de un nuevo virus, solamente se podrían detectar, analizar y desinfectar unos 250 por año. Eso quiere decir que más virus significa también más trabajo para los desarrolladores.

Además, todos estos nuevos virus eran similares unos a otros, provocando errores de identificación, y por lo tanto una desinfección ineficaz. Muchos escáneres fallaban en la clasificación del virus en cuestión. La mayoría de los virus procedían de Europa del Este y Rusia, pero en Bulgaria se localizó otro importante foco de producción de códigos malignos. Enseguida muchos países se unieron a la nefasta carrera de producción de virus: Alemania con 'Gonorrea', Suecia con 'Demoralised Youth', Estados Unidos con 'Hellpit', Reino Unido con 'Dead on Arrival' y 'Semaj'. Algunos de estos virus jamás salieron del laboratorio, pero contribuyeron a extender la fama de estos códigos por todo el mundo, animando a los creadores de virus a ser cada vez más productivos. La rapidez de creación produjo el efecto de contribuir al plagio: cualquier creador de virus no tenía más que descargar código fuente y efectuar en él unos cuantos cambios.

1991 fue también el año de los virus polimórficos que tuvieron un gran impacto sobre los usuarios. En abril de 1991, 'Tequila' recorrió el mundo de parte a parte. Fue escrito en Suiza, y fue robado al autor por un amigo, que lo introdujo en los equipos informáticos de su padre. El padre era un vendedor de software, y así fue como 'Tequila' se difundió ampliamente.

Se trató del primer virus polimórfico difundido a escala mundial. En mayo, los nuevos motores de búsqueda lo detectaban, pero no fue hasta septiembre que se empezó a reducir su expansión. Si no se desinfectaba totalmente existía un riesgo de pérdida de un 1 por

ciento de los archivos, y esto se incrementaba cada vez que se detectaba el virus pero no se desinfectaba de forma efectiva.

En septiembre de 1991 el virus 'Maltese Amoeba' hizo de las suyas por toda Europa. Se trataba de otros virus polimórfico que provocó la aparición de una docena de variantes antes de fin de año, todos clasificadas como 'de difícil erradicación'. En este año se anunció la inmediata aparición de un virus que podía tomar nada más y nada menos que 4 billones de formas diferentes, pero esto sucedería ya para 1992, y no se trataba de un virus.

- **1992: Un año lleno de incidencias**

Enero de 1992 fue el año de la aparición de la 'Self Mutating Engine(MtE) de Dark Avenger. En principio, la comunidad mundial pensó que se trataba de un nuevo virus, de nombre 'Dedicated', pero después hizo aparición la MtE. Apareció como un archivo OBJ, con el código fuente de un simple virus e instrucciones para enlazar el archivo OBJ a un virus, de tal manera que, al final, se podía obtener un virus polimórfico.

Inmediatamente, los cazadores de virus se pusieron a la tarea de desarrollar detectores para la MtE. Cada compañía estableció, para hacer frente a la amenaza, diferentes tipos de estrategia: unas se preocuparon por desarrollar soluciones para detener el código maligno, mientras que otras decidieron ignorarlo con la secreta esperanza de que no fueran afectadas. En un principio, se creyó que habría cientos y cientos de virus haciendo uso de MtE, ya que era muy fácil de usar y permitía a dichos virus ocultarse de forma extraordinaria. Pero los creadores de virus se dieron cuenta rápidamente de que un escáner que fuera capaz de detectar un MtE podía detectar todos.

A la MtE le siguió 'Commander Bomber', también de 'Dark Avenger'. Antes de 'Commander', uno podía prever fácilmente en qué archivo estaba oculto un virus. Muchos desarrolladores de productos aprovechaban esta facilidad para crear rápidamente herramientas anti-virus. Pero 'Commander Bomber' cambió esto, de tal manera que los escáneres se veían obligados a chequear todos los archivos, o bien localizar el virus mediante un seguimiento completo del código. Otro virus importante que surgió durante este periodo fue 'Starship'. Se trata de un virus completamente polimórfico, que constaba de una serie de trucos anti-debbuging y anti-checksumming. Los programas de 'checksumming' sirven para detectar un virus en función de que posee código ejecutable que muta para replicarse. 'Starship' solamente infectaba los archivos cuando éstos eran copiados desde el disco duro al disquete. Por lo tanto, los archivos residentes en el disco duro no cambiaban nunca. Pero la copia del disquete estaba infectada, por lo que si este disquete se introducía en otro equipo y se chequeaba el sistema por medio del 'checksummer', éste lo aceptaba sin problemas. El virus 'Starship' se instalaba a sí mismo en el disco duro, pero sin hacer ningún cambio en el código ejecutable. Cambiaba los datos, eso sí, de partición, efectuando una nueva partición en el 'boot'. Esta nueva partición contenía el código del virus, que se ejecutaba antes de pasar el control a la partición 'boot' original.

Probablemente, el virus más importante durante 1992 fue el conocido 'Michelangelo'. Uno de los más conocidos vendedores de productos anti-virus norteamericano dio la alerta: cerca de cinco millones de PC's podían venirse abajo el 6 de marzo de este año. En muchas empresas cundió el pánico, cuando los medios de comunicación se hicieron eco de este asunto. Sin embargo, el 6 de marzo sólo tuvieron problemas entre 5,000 y 10,000 equipos

informáticos, y naturalmente los vendedores de software tuvieron que moderar el ímpetu de sus avisos de alarma. Probablemente, nunca llegaremos a saber cuánta gente, en realidad, se vio afectada por 'Michelangelo', pero lo cierto es que en los días previos al 6 de marzo la mayoría de los usuarios llevaron a cabo exhaustivos exámenes de sus equipos en pos del virus. Después de esta fecha, muchos expertos en virus de todo el mundo vieron como sus opiniones, siempre tenidas en cuenta, eran objeto del más absoluto desprecio.

En Agosto aparecieron los primeros paquetes de virus de autor. Primero apareció el VCL ('Virus Creation Laboratory'), de 'Nowhere Man', y a continuación 'Dark Angel' generó el 'Phalcon/Skism Mass-Producer Code Generator'. Estos paquetes hicieron posible que cualquier persona pudiera hacer uso de un PC para escribir su virus personal. En el transcurso de un año, aparecieron, en consecuencia, docenas de nuevos virus en el mercado, todos ellos creados mediante el uso de estas herramientas.

A finales de 1992 un nuevo grupo de creadores de virus, ARCV (Asociación de Virus Auténticamente 1992 Crueles) apareció en el Reino Unido, y al cabo de un par de meses, la Unidad de Crimen Computacional de Scotland Yard los localizó y arrestó, gracias a la inestimable ayuda de la comunidad de expertos en soluciones anti-virus. El efímero florecimiento de la ARCV duró sólo tres meses, durante los cuales crearon unas cuantas docenas de nuevos virus y reclutaron a algunos miembros para su causa particular.

Otro de los hechos destacables en este año tan movido fue la aparición de personas que se dedicaban a la venta de colecciones de virus. Para ser más precisos, se trataba realmente de colecciones de archivos, algunos de los cuales eran virus. En los Estados Unidos, John Buchanan ofreció su colección de unos cuantos miles de códigos al precio de 100 dólares por copia, y en Europa, la Unidad Clínica de Virus sacó a la venta varias colecciones por 25 dólares la copia.

- **Hasta el año 2001**

A principios de 1993, XTREE anunció que iban a abandonar el negocio del software anti-virus. Era la primera gran compañía que renunciaba a la lucha. Casi al mismo tiempo, un nuevo grupo de creadores de virus hizo su aparición en Holanda: su nombre, 'Trident'. El principal creador de virus de este grupo, Masouf Khafir, elaboró una máquina polimórfica denominada, precisamente, 'Trident Polymorfic Engine', y lanzó un virus que la utilizaba llamado 'GIRAFE'. A esto, le siguieron varias nuevas versiones de TPE. Este virus es mucho más difícil de detectar que el MtE, y mucho más difícil de evitar sus falsas alarmas.

Khafir también lanzó el primer virus que trabajaba de acuerdo con un principio que ya fue enunciado por Fred Cohen. El virus 'Cruncher' era un código maligno de compresión que automáticamente se incluía en archivos para autoinstalarse en tantos equipos como fuera posible.

Mientras tanto, 'Nowhere Man' y el grupo 'Nuke' había estado, también, bastante ocupados. A principios de este mismo año, fue lanzado el 'Nuke Encryption Device (NED). Se trataba de otro mutador mucho más difícil de neutralizar que MtE. El virus consiguiente, 'Itshard', pronto siguió a la aparición de esta nueva máquina polimórfica.

También 'Dark Angel' quiso apuntarse a la moda del polimorfismo. Este creador de virus lanzó DAME ('Dark Angel's Multiple Encryptor Device (NED)'). Se trataba de otro mutador cuyo virus era 'Trigger'. Este código relanzó la versión 1.4 de TPE (de nuevo, era mucho más complejo y difícil de erradicar que en las versiones previas), y lanzó un virus llamado 'Bosnia' que lo utilizaba.

Un poco después de esta oleada de códigos polimórficos, Lucifer Messiah, de Anarkick Systems, había tomado la versión 1.4 de TPE y escrito un virus llamado 'POETCODE', utilizando una versión modificada de esta máquina (la 1.4b).

Pero el más famoso de los polimórficos que aparecieron a principios de 1993 fue 'Tremor', el cual ascendió rápidamente a las alturas de la fama cuando fue difundido a través de un show de la televisión alemana dedicado precisamente a las novedades del software. El archivo infectado fue PKUNZIP.EXE, que la mayoría de los receptores usaban para descomprimir archivos adjuntos al correo.

A mediados de año, el grupo 'Trident' aumentó su preeminencia con la entrada de Dark Ray y John Tardy en el grupo. Tardy había lanzado un virus completamente polimórfico de 444 bytes, y todos los expertos estaban pendientes del grupo, en espera de nuevas y malignas creaciones, posiblemente de rango superior. Lo peor que tuvo lugar en este fatídico año fue la emergencia de un creciente número de paquetes de virus de autor y máquinas polimórficas, que hacían más fácil escribir virus que los escáneres encontraban difíciles de detectar.

También en 1993 desaparecieron muchas importantes empresas desarrolladoras de software anti-virus, como Certus (uno de cuyos productos más representativos era Novi) ó Fifth Generation (creadores del producto 'Untouchable'). No obstante, también hubo algunas buenas noticias: la empresa S&S International recibió el galardón 'Queen's Award for Technological Achievement'. Este premio se otorgó por el lenguaje de descripción de virus VIRTRAN, que es la base fundamental de FindVirus y VirusGuard.

Los siguientes años conocieron una superabundancia de virus escritos por medio de paquetes, lo cual causó enormes dificultades a los desarrolladores de software anti-virus. Se hizo, de repente, necesario mecanizar los procesos de análisis de códigos malignos. La solución fue la GDE ('Máquina de Desciframiento Genérico'), que descifraba el código de un archivo sospechoso, permitiendo así llegar a la conclusión de si se trataba o no de un virus. Esto eliminaba el peligro de las falsas alarmas, ya que una vez que un virus es descifrado, se facilita muchísimo el proceso de una identificación positiva del citado virus. `

En abril del año 1994, la firma Central Point Software dejó de existir. Central Point llegó a ser uno de las principales empresas del mercado de los desarrolladores de soluciones anti-virus, con su producto CPAV. En este mismo año también aparecieron muchas máquinas polimórficas y nuevos virus, como 'SMEG', que fue lanzado por su autor como 'Smeg.Pathogen' y 'Smeg.Queeg'. Debido a que estos virus se difundieron inmediatamente después de su creación, supusieron una especie de curioso test que denotaba la capacidad de reacción de las empresas desarrolladoras de anti-virus.

El 26 de marzo de 1996, Chrisopher Pile, de 26 años, oriundo de Plymouth (en Inglaterra), fue condenado de acuerdo con la ley de Utilización Errónea de Equipos Informáticos en conexión con la aparición y posterior difusión de los virus 'Smeg'.

La aparición de nuevos tipos de virus, así como, por desgracia, su amplia difusión hace imposible la inclusión en este apartado de todos ellos. Es por esto por lo que a continuación hacemos una breve referencia a aquellos virus y métodos de propagación más destacables:

1996 - Boza, Concept, Laroux, & Staog: Boza es el primer virus diseñado específicamente para ficheros de Windows 95. Concept es el primer virus de Macro para Word. Laroux es el primer virus de macro para Excel. Staog es el primer virus para Linux (realizado por los autores del Boza).

1998 - Strange Brew & Back Orifice: Strange Brew es el primer virus para Java. Back orifice es el primer virus Troyano diseñado para la administración remota de equipos, es decir, permite tomar el control de una maquina remota por otro usuario vía Internet.

1999 - Melissa, Corner, Tristate, & Bubbleboy: Melissa es la primera combinación entre un virus de macro de Word y un gusano que usa la libreta de direcciones del Outlook y del Outlook Express para enviarse a otros vía E-mail. Corner es el primer virus que infecta ficheros MS Project. Tristate es el primer virus de macro multi-programa; infecta ficheros de Word, Excel, y de PowerPoint. Bubbleboy es el primer gusano que puede activarse cuando un usuario abre un mensaje en Microsoft Outlook. No necesita un fichero adjunto. Bubbleboy era la prueba del concepto que luego utilizo el virus Kak ampliamente difundido gracias a esta técnica.

2000 - DDoS, Love Letter, Liberty (Palm), Streams, & Pirus: DDoS fue el mayor denegador de servicios que atacó cerrando importantes sitios web, tales como Yahoo!, Amazon.com, y otros. El virus Love Letter, se convirtió en el gusano que mas rápido infecto a los usuarios; tirando los servidores de correo alrededor del mundo. En Agosto de 2000 apareció el primer Troyano desarrollado para la Palm PDA. Llamado Liberty y desarrollado por Aaron Ardiri , uno de los desarrolladores del emulador de la consola Game Boy para la Palm. Liberty, fue desarrollado como un programa de desinstalación y fue distribuido a unas pocas personas para ayudarles a controlar a aquellas personas que intentasen robarles su software. Cuando fue accidentalmente puesto en circulación, Ardiri ayudo a contener esta infección. Streams comenzó siendo la prueba de concepto de virus para el subsistema de ficheros del sistema de ficheros NTFS, llamado Alternate Data Stream (ADS) que permite incluir datos adicionales unidos al fichero de origen. Como prueba de concepto, Streams no debe propagarse pero como en otros casos estamos expectantes. Pirus es otra prueba de concepto, es un script escrito en PHP. Intenta añadirse a ficheros HTML o PHP. Pirus fue descubierto el 9 de Noviembre de 2000.

2001- Ramen, Nimda, Sircam. Aparece el primer virus para servidores web Linux: Ramen. El gusano Ramen comienza a atacar sistemas Linux en Enero de 2001. Debido a la amplia implantación de este sistema operativo en el mundo Internet, este virus se propago rápidamente, pero sin causar grandes destrozos.

El virus más propagado este año es el Nimda, que llega en un fichero adjunto a un correo electrónico que es capaz de autoejecutarse aprovechando una vulnerabilidad del Internet Explorer. Otro virus que también alcanzó gran difusión (y que aún sigue teniéndola) es el Sircam. Utiliza su propio motor SMTP para propagarse a otros ordenadores.

En total, se estima que las pérdidas producidas por los virus informáticos durante este año ascienden en todo el mundo a 2 billones y medio de pesetas (algo menos que en el año 2000, cuando el famoso virus "I love you" causó, él sólo, cerca de 2 billones de dólares de pérdidas).

- **El año 2002**

Klez

El virus "estrella" de este año es el virus Klez (en sus variantes F, I, G o H). Este virus explota una vulnerabilidad en el Internet Explorer por la cual es capaz de autoejecutarse con solo visualizar el correo electrónico en el que llega como adjunto. El virus es capaz de impedir el arranque del sistema y de inutilizar ciertos programas. En abril comenzó a difundirse este gusano, y a su rápida propagación a través de e-mail hay que añadir otras complicaciones, entre ellas sus técnicas de camuflaje (cambios continuos en remitente y asunto) y que envía ficheros personales aleatoriamente a terceras personas. En mayo el virus llegó a propagarse tanto que casi uno de cada 300 correos estaban infectados. La empresa de seguridad MessegeLabs afirma de él que es el peor virus de la historia.

Bugbear

Este virus apareció en septiembre. Según Sophos afectó a millones de ordenadores en todo el mundo, y Panda ha afirmado que uno de cada cinco PCs en España han tenido problemas con él. Este gusano, si no es detectado a tiempo, destruye la protección antivirus.

Frethem, Simile

Son los primeros virus híbridos que han aparecido, capaces de atacar tanto sistema Linux como Windows. Frethem es un gusano muy engañoso que suele tener como asunto "Re: Your password!". Es muy fácil infectarse con él, ya que el virus se activa automáticamente con la previsualización del mensaje en el Outlook Express.

Sircam, Nimda, Badtrans

Estos virus ya habían aparecido en el 2001, pero a lo largo de este año han seguido causando estragos. El método de propagación preferido de los virus informáticos durante este año continúa siendo el correo electrónico. El número de mensajes enviados asciende ya a unos 10,000 millones de correo diarios en todo el mundo. Este tráfico intenso, unido a que muchos virus viajan en atractivos correos (con supuestas promesas de amor, información ofrecida, bonitos protectores de pantallas, etc.) explica que la mayoría de los virus elijan esta vía para propagarse. Según nuestras estadísticas, entre el 1% y el 2% de los correos que se reciben diariamente están infectados con uno o más virus. Además, y especialmente este año, cada vez son más los virus que utilizan populares herramientas de compartición de ficheros en Internet (como KaZaa) para propagarse de un ordenador a otro.

En la actualidad, en general, casi cualquier herramienta que se use como medio de comunicación en Internet es aprovechada por los virus para propagarse: MSN Messenguer, chats IRC, ICQ, etc...

4.1.3 ¿Qué son los virus?

Son programas que se introducen en nuestros ordenadores de formas muy diversas. Este tipo de programas son especiales ya que pueden producir efectos no deseados y nocivos. Una vez que el virus se haya introducido en el ordenador, se colocará en lugares donde el usuario pueda ejecutarlos de manera no intencionada. Hasta que no se ejecuta el programa infectado o se cumple una determinada condición, el virus no actúa. Incluso en algunas ocasiones, los efectos producidos por éste, se aprecian tiempo después de su ejecución (payload).

4.1.4 ¿Qué elementos infectan los virus?

Los ficheros que se encuentran en un medio de almacenamiento como los discos duros o disquetes. Más concretamente serán infectados todos aquellos archivos, ficheros o documentos (los tres términos indican el mismo concepto, en general) que tengan la característica de ser programas. Un programa no es más que un fichero cuya extensión es EXE o COM, que se puede ejecutar para que realice determinadas operaciones.

También existen virus que se encargan de infectar ficheros que no son programas. No obstante, estos ficheros contendrán elementos, denominados macros, incluidos en ellos. Estas macros son programas que el usuario puede incluir dentro de un determinado tipo de archivos. Otro suelen atacar a los propios medios de almacenamiento. De esta forma, atacando a los lugares en los que se guardan ficheros, el daño provocado afectará a toda la información contenida en ellos.

4.1.5 Medios de entrada más habituales para los virus

Los virus utilizan los siguientes medios para ello:

- **Unidades de disco extraíbles:** las unidades de disco son aquellos medios de almacenamiento en los que se guarda información, mediante ficheros, documentos o archivos. Con ellos se puede trabajar en un ordenador para, posteriormente, utilizarlos en otro diferente. Algunos de estos medios de almacenamiento pueden ser los disquetes, CD-ROMs, unidades Zip y Unidades Jazz.
- **Redes de ordenadores:** Una red es un conjunto o sistema de ordenadores conectados entre sí físicamente, para facilitar el trabajo de varios usuarios. Esto quiere decir que existen conexiones entre cualquiera de los ordenadores que forman parte de la red, pudiendo transferirse información entre ellos. Si alguna de esta información transmitida de un ordenador a otro estuviese infectada, el ordenador en el que se recibe será infectado.
- **Internet:** Cada día más se utilizan las posibilidades que brinda Internet para obtener información, realizar envíos y recepciones de ficheros, recibir y publicar noticias, o descargar ficheros. Todas estas operaciones se basan en la transferencia de información, así como en la conexión de diferentes ordenadores en cualquier parte del mundo. Por tanto, cualquier virus puede introducirse en nuestro ordenador al mismo

tiempo que la información recibida. A través de Internet la infección podría realizarse empleando diferentes caminos como los siguientes:

- **Correo electrónico:** En un mensaje enviado o recibido se pueden incluir documentos o ficheros (fichero adjunto o anexado, "attached"). Estos ficheros podrían estar infectados, contagiando al ordenador destinatario.
- **Páginas Web:** Las páginas que visitamos en Internet son ficheros de texto o imágenes escritos en un lenguaje denominado HTML. No obstante también pueden contener programas denominados Controles ActiveX y Applets de Java que son programas. Estos sí pueden estar infectados y podrían infectar al usuario que se encuentre visitando esa página.

4.1.6 Tipos de virus

Los diferentes virus que existen se pueden clasificar dependiendo del medio a través del cual realizan su infección y las técnicas utilizadas para realizarla. Aunque, bastantes de ellos tendrán una característica especial por la que se asociarán a un tipo concreto dentro de esta clasificación, otros podrán formar parte de varios grupos diferentes.

- **Virus de Fichero:** Este tipo de virus se encarga de infectar programas o ficheros ejecutables (archivos con extensiones EXE o COM). Al realizar la ejecución de uno de estos programas, de forma directa o indirecta, el virus se activa produciendo los efectos dañinos que le caractericen en cada caso. La mayoría de los virus existentes son de este tipo, pudiéndose clasificar cada uno de ellos en función de su modo de actuación.
  - **Virus Residentes:** Cuando se ponen en marcha, la primera acción que realizan consiste en comprobar si se cumplen todas las condiciones para atacar (fecha, hora,... etc.). De no ser así, se colocan en una zona de la memoria principal, esperando que se ejecute algún programa. Si en alguna de las operaciones que realiza el sistema operativo se trabajase con un fichero ejecutable (programa) no infectado el virus lo infectará. Para ello, el virus se añadirá al programa que infecta, añadiendo su código al propio código del fichero ejecutable (programa).
  - **Virus de Acción Directa:** En el momento de su ejecución, el virus trata de replicarse a sí mismo. Esto implica que creará copias de sí mismo. Cumpliéndose unas determinadas condiciones, propias en cada caso, se activará pasando a realizar infecciones dentro del directorio o carpeta en el que nos encontremos y dentro de los directorios que se encuentran especificados en la línea PATH (camino o ruta de directorios) dentro del fichero AUTOEXEC.BAT (este fichero se encuentra siempre en la raíz del disco duro, siendo un fichero de proceso por lotes que realiza ciertas operaciones cuando se enciende el ordenador). Es posible llevar a cabo la desinfección, de los ficheros afectados por el virus, dejándolos en un estado correcto.
  - **Virus de Sobreescritura:** Este tipo de virus se caracteriza por no respetar la información contenida en los ficheros que infecta, haciendo que estos queden inservibles posteriormente. Pueden encontrarse virus de sobreescritura que además son residentes y otros que no lo son. Aunque la desinfección es posible, no existe posibilidad de recuperar los ficheros infectados, siendo la única alternativa posible la eliminación de éstos.
  - **Virus de Compañía:** Para efectuar sus operaciones de infección, los virus de compañía pueden esperar en la memoria hasta que se lleve a cabo la ejecución

de algún programa (virus residentes) o actuar directamente haciendo copias de sí mismos (virus de acción directa). Al contrario que los virus de sobreescritura o los residentes, los virus de compañía no modifican los ficheros que infectan. Cuando el sistema operativo está trabajando (ejecutando programas, ficheros con extensiones EXE y COM) puede ocurrir que éste, el S.O., tenga que ejecutar un programa con un nombre determinado. Si existen dos ficheros ejecutables con el mismo nombre pero con diferentes extensiones (uno con extensión EXE y otro con extensión COM), el sistema operativo ejecutará en primer lugar el que lleve la extensión COM.

Esta peculiaridad del sistema operativo es aprovechada por los virus de compañía. En caso de existir un fichero ejecutable con un determinado nombre y extensión EXE, el virus se encargará de crear otro fichero con el mismo nombre pero con extensión COM haciéndolo invisible (oculto) al usuario para evitar levantar sospechas. Este fichero que crea será el propio virus y el sistema operativo, al encontrarse con dos ficheros que llevan el mismo nombre, ejecutará en primer lugar el de extensión COM, siendo éste el virus que en ese preciso instante realizará la infección. Tras realizarse la ejecución del fichero COM correspondiente al virus, éste devuelve el control al sistema operativo para que ejecute el fichero EXE. De esta forma el usuario no tendrá conocimiento de la infección que en ese preciso instante ha tenido lugar.

- **Virus de Boot:** El término Boot o Boot Sector representa lo que también se denomina "sector de arranque". Se trata de una sección muy importante en un disco (disquete o disco duro), en la cual se guarda la información sobre las características de ese disco, además de incluir un programa que permite arrancar el ordenador con ese disco, determinando previamente si existe sistema operativo en el mismo.

Este tipo de virus de Boot, no afectan a los ficheros por lo que el contenido del disco no estará en peligro a no ser que se intente arrancar el ordenador con ese disco. Si esto ocurre, el virus realizará la infección siguiendo una serie de pasos habituales:

1. Reserva un determinado espacio en memoria para que éste no sea ocupado por ningún otro programa.
2. Después de hacer esto, se coloca en esa zona reservada de la memoria.
3. Desde esa posición de memoria se encarga de interceptar servicios que realiza el sistema operativo. En cada ocasión que una aplicación del S.O. llame a una función de acceso a ficheros, el virus toma el control. De esta forma comprueba si el disco al que se accede esta infectado y si no lo está, lo infecta.
4. Una última operación que realiza es volver a colocar el sector de arranque original (sin infectar), cediéndole el control, de tal forma que parezca no haber ocurrido nada. No obstante el virus seguirá actuando.
5. Las infecciones de virus de Boot se suelen realizar mediante disquetes siendo la protección contra escritura en él, el mejor método de protección.

- **Virus de Macro:** A diferencia de los tipos de virus comentados anteriormente, los cuales infectan programas (ficheros EXE o COM) o aplicaciones, los virus de macro realizan infecciones sobre los ficheros que se han creado con determinadas aplicaciones o programas. Con ellos es posible crear documentos de texto, bases de datos, hojas de cálculo,...etc. Cada uno de estos tipos de ficheros puede tener

adicionalmente unos pequeños programas, denominados macros. Una macro no es más que un micro-programa que el usuario asocia al fichero que ha creado con determinadas aplicaciones y que no depende del sistema operativo sino de acciones determinadas que el usuario puede realizar dentro del documento que la contiene. Mediante ellos es posible automatizar conjuntos de operaciones para que se lleven a cabo como una sola acción del usuario de forma independiente sin necesidad de realizarlas una a una manualmente.

Pues bien, estas macros son susceptibles de infección, lo que significa que los virus (más concretamente los de macro) pueden fijar sus objetivos de infección en ellas. En este caso, al abrir un documento que contenga macros, éstas se cargarán de forma automática (ejecutándose o esperando que el usuario decida ejecutarlas). En ese instante o posteriormente, el virus actuará realizando cualquier tipo de operación perjudicial. A la diferencia de lo que se piensa habitualmente, los virus de macro pueden realizar acciones dañinas de bastante importancia, propagándose en poco tiempo de forma muy rápida.

- **Virus de enlace o de directorio:** Los ficheros son los documentos que contienen la información real en la que se ha trabajado (textos, bases de datos, hojas de cálculo, imágenes, sonido,... etc.) o programas (extensiones EXE y COM) y otros tipos de "elementos" que hacen posible la ejecución de éstos. Cuando hablamos de un fichero, podemos emplear indistintamente éste término, o el de documento, o el de archivo. Para organizar toda esta información, se crean directorios o carpetas que son quienes contienen a los ficheros, pudiendo contener también otras carpetas o directorios (subcarpetas o subdirectorios). De esta forma, la estructura de un disco se puede ver como una gran carpeta clasificadora en la que los ficheros son guardados en determinadas secciones (directorios o carpetas). Otra forma diferente de presentar este concepto es pensar que el disco es una mesa de despacho en la que tenemos cajones. Estos cajones son los directorios, dentro de los cuales guardamos hojas (que representarían a los documentos, ficheros o archivos), pero que también pueden contener subsecciones (subcarpetas o subdirectorios). En definitiva el documento, fichero o archivos es el contenido y las carpetas o directorios son el continente que alberga dicho contenido.

Pues bien, el sistema informático deberá conocer en todo momento información sobre un determinado fichero, como el nombre que tiene y el lugar (carpeta o directorio) en el que se encuentra (en el que se ha guardado). Para ello le asignará una dirección a la que se debería acceder en caso de desear utilizar ese determinado fichero.

Los virus de enlace o directorio se encargan de alterar estas direcciones para provocar la infección de un determinado fichero. Si un programa (fichero EXE o COM) se encuentra en una dirección concreta, para ejecutarlo habrá que acceder a dicha dirección. Sin embargo, el virus la habrá modificado con anterioridad. Lo que hace es alterar esta dirección para que apunte al lugar en el que se encuentra el virus, guardando en otro lugar la dirección de acceso correcta. De esta forma, cuando se pretenda ejecutar el fichero, lo que se hará realmente es ejecutar el virus.

Ya que este tipo de virus puede modificar las direcciones donde se encuentran todos los ficheros del disco (disco duro), su capacidad para infectar TODOS éstos es real. De este

modo, los virus de enlace o directorio pueden infectar toda la información contenida en un disco, pero les es imposible realizar infecciones en unidades de red o agregarse a los ficheros infectados. En caso de realizar un análisis del disco en busca de errores (mediante programas como SCANDISK o CHKDSK), se detectarán grandes cantidades de errores que identifican todos los enlaces a los ficheros que el virus ha modificado. No obstante, en este caso sería mejor no recuperarlos ya que podría producirse un caos en lo que al sistema de almacenamiento de la información se refiere, que sería más perjudicial.

4.2 El Correo Basura o Spam

4.2.1 Introducción

Uno de los grandes problemas que afronta actualmente Internet es la proliferación de correo basura, correo no solicitado y que no aporta ningún beneficio al receptor. Según algunas estadísticas es ya la mitad de todo el correo electrónico de Internet, y hasta el 80%, según la empresa especializada **MAPS**. El proyecto **Sanet** recoge estadísticas de correo basura en la comunidad académica de **RedIRIS**.

El correo basura **cuesta dinero**, tanto por el tiempo que se pierde examinándolo, como por los recursos de *hardware* y *software* necesarios para manejarlo (ancho de banda, servidores de correo más potentes, software de filtrado, etc.), costes que deben ser soportados por las organizaciones en forma de inversiones y horas de trabajo de sus empleados, y que en el caso de los proveedores de acceso a Internet, acabarán repercutiendo a los clientes.

Este correo tienen diversas fuentes, desde los virus (y mensajes de antivirus enviados a remitentes falsificados por virus) a los mensajes con bultos que son reenviados por muchos usuarios. No obstante, el tipo más problemático es el llamado **spam,** también referido a menudo como **correo comercial no solicitado** (aunque no tiene por qué ser comercial). El término "spam", debido a su difusión, es usado con varios sentidos, pero aquí nos quedaremos con la definición más habitual en los círculos que lo combaten.

4.2.2 Definición de Spam

Se considera un mensaje electrónico "Spam" si:

1. Se envía de manera masiva y automatizada, sin atender a la identidad ni al contexto del receptor.
2. El receptor no ha solicitado o permitido expresamente de forma verificable el envío del mensaje. Por ejemplo, marcando una casilla de verificación claramente visible en una formulario Web y donde se explique con claridad la temática de los mensajes que se enviarán.
3. La transmisión y recepción del mensaje proporciona al remitente un beneficio desproporcionado. El receptor recibe un mensaje poniendo sus medios: su ancho de banda y su ordenador, similares a los que usa el remitente para enviar el mensaje a miles de buzones, y establece una comunicación que interesa fundamentalmente al remitente. Normalmente esto se concreta en hacer una campaña publicitaria a un precio ínfimo, pero también sería Spam.

El origen del término Spam es muy curioso. SPAM (*SPiced hAM*) es una marca de jamón enlatado bastante difundida en EE.UU. y de no muy alta calidad. Parece ser que el uso en jerga informática fue inspirado por un *sketch* de Monty Python, en el que una pareja va a cenar a un restaurante donde todos los platos tienen spam. Mientras el camarero les explica la carta, un grupo de vikingos empieza a corear frases como "spam, spam, spam, spam, lovely spam" en varias ocasiones y cada vez más alto, hasta que es lo único que se oye.

4.2.3 ¿Por qué se envía tanto Spam?

Es un negocio. La mayor parte de estos mensajes son campañas de publicidad engañosas (como productos milagrosos) fraudulentas (por ejemplo, colecciones de programas pirateados) o productos de baja calidad paro los que no es rentable una campaña publicitaria convencional. La mayoría de los usuarios los perciben como tales, y aunque se estima que la tasa de respuesta es ínfima (menos de 15 por millón), debido al bajísimo coste que tienen, es suficiente para producir beneficios. Hay muchos individuos y empresas que soportan esta práctica y hay abundante información sobre cómo hacer spam en Internet.
Aunque se hacen esfuerzos técnicos para dificultarles su labor, los *spammers* (individuos u organizaciones que envían spam) no permanecen pasivos y utilizan numerosas técnicas y trucos desarrollados en los últimos años para seguir entregando sus correos. Estas incluyen:

- Utilizar una dirección distinta para cada envío y abandonarla o eliminarlas después
- Falsificar las cabeceras de los mensajes de correo electrónico para dificultar el rastreo del origen.
- Infiltrarse en servidores de correo legítimos (reventarlos) y usarlos como fuente de envío.
- Utilizar troyanos, como la familia Mitglieder, que instalan relés SMTP en el PC infectado, y que pueden ser usados para reenviar spam.
- Deformación de palabras de los mensajes (por ejemplo cambiando letras por números, o insertando espacios y puntos aleatoriamente) para engañar a los filtros de palabras.

4.2.4 ¿Cómo luchar contra el Spam?

Prevención: como en tantas otras cosas, más vale prevenir que curar. Los consejos básicos son:

- Utilice al menos dos direcciones de correo electrónico (o un alias). Una para sus contactos más importantes, y otra (u otras) para dar en sitios web o listas de correo, de forma que si empieza a recibir mucho correo basura pueda desechar esa dirección.
- Evite que su dirección de correo aparezca en sitios web, donde son muy fáciles de capturar, especialmente si se usan enlaces de tipo *mailto:*.
- Procure no participar en mensajes encadenados (como bulos) que son remitidos masivamente a numeroso destinatarios en el campo "Para". Recomiende a sus contactos que usen el campo "CCO" (Con Copia Oculta) o que usen listas de distribución de correo.
- Nunca responda al spam, a no ser que esté convencido de de que proviene de una fuente seria. La dirección del remitente suele ser falsa, así que si devuelve el correo,

probablemente le llegue a alguien que no tenga nada que ver. Las instrucciones para no recibir más mensajes similares también suelen ser falsas, y normalmente lo único que se consigue es confirmar al *spammer* que la cuenta está activa y recibirá más correo basura. Y por supuesto, no adquiera nunca productos anunciados mediante spam para no sustentar estas prácticas.

- Utilización de filtros anti-spam. Se han desarrollado numerosos programas que usan varias técnicas para separar el correo basura del deseado. Son medidas paliativas, que no atacan directamente la raíz del problema, pero al menos ahorran al usuario el tiempo de hacerlo manualmente.

Hay otros filtros de tipo heurístico, que buscan contenidos típicos de spam, como formularios HTML o identificadores únicos en el mensaje: Mozilla y derivados, SpamCombat, Spamihilator, SpamAssassin, etc.

4.3 Los Programas Espía o *Spywares*

Son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad. Todas estas acciones se enmascaran tras confusas autorizaciones al instalar terceros programas, por lo que rara vez el usuario es consciente de ello.

4.3.1 ¿Cómo funcionan?

Los programas espía pueden instalarse en un ordenador mediante un virus, un troyano, o bien, como generalmente ocurre, estar ocultos en la instalación de un programa gratuito (*freeware* o *adware*). Estos últimos programas permiten al usuario la descarga y uso de su *software* sin pagar, con la condición de soportar la publicidad insertada en ellos, pero algunos también introducen *spywares* para recopilar valiosa información de nuestros hábitos de navegación, sin que nosotros tengamos conocimiento de ello.

La información que recopilan los programas espías suele tener un uso estadístico y comercial, valioso para las empresas de publicidad. Pero estos programas pueden, y algunos lo hacen, acceder del mismo modo a información personal que tengamos almacenada (nombre, dirección de correo electrónico...) o incluso a datos vitales como cuentas de usuario y contraseñas. Otro de los efectos de los spywares más intrusivos es el de cambiar nuestra página de inicio a otra a elección del programa espía, la cual puede ser una página en blanco, erótica o de contenido dudoso. Si se intenta restaurar la página de inicio desde las opciones del explorador se verá que esto no es posible. Los cambios que el espía ha realizado en el registro del sistema no lo permiten. Esta actividad es conocida como "*Secuestro del Navegador*".

Sin embargo, no hay que confundir los programas espías con virus, troyanos, gusanos, etc. Ya que estos últimos se dedican a dañar, de una forma u otra, el equipo infectado. Los programas espías por el contrario se dedican a recopilar ilegalmente información referente al usuario que utiliza el equipo; por ejemplo, páginas en las que navega, qué cosas suele comprar por Internet, *software* instalado en el sistema, antivirus utilizado… Toda esta información la recopilan ejecutando la aplicación de forma invisible para

el usuario pero consumiendo recursos, por lo que ralentizan la velocidad del ordenador y la conexión a Internet.

4.3.2 ¿Quién se beneficia?

Las empresas que los incluyen en su *software* argumentan que los datos que recopilan son anónimos y usados sólo con fines estadísticos, además, es un beneficio para que puedan seguir elaborando *software* gratuito, por el que de otro modo tendrían que cobrar. El problema viene porque no se informa claramente al usuario de la inclusión en el software gratuito de este tipo de programas, ni de la información que se va a obtener de él. Por otro lado si se desinstala un espía, es probable que la aplicación con la cual venía deje también de funcionar. Por el contrario, si se desinstala este *software* gratuito para acabar con la fuga de datos, no se consigue el objetivo de desinstalar el *spyware*, que seguirá en el ordenador recopilando y enviando información.

4.3.3 ¿Qué hacer?

La solución para evitar esta fuga de información de nuestro equipo pasa por usar programas antiespías. Tienen un funcionamiento similar a los programas antivirus, pero analizan el sistema en busca de programas espías y los eliminan. Estos programas no son incompatibles con los programas antivirus, sino que son complementarios. Teniendo ambos instalados en nuestro ordenador estaremos mejor protegidos contra posibles intrusiones en nuestro sistema. A continuación se dan algunos programas "Antispy" gratuitos que puede ayudar a controlar este problema.

4.3.4 Herramientas Anti-espías

- **En español**

Ad-aware SE Personal: Programa antiespías gratuito para uso particular. Con posibilidad de actualización por Internet y ampliable mediante complementos. Intuitivo y fácil de usar. Tiene capacidad de eliminación de los programas espías encontrados. La versión comercial también tiene capacidad residente ("Ad-Watch"). Válido para todos los Sistemas Operativos Windows. Para que la interfaz de Ad-Aware se muestre en español hay que descargar e instalar Ad-Aware SE (Standard Edition) y el paquete de idiomas (language pack) de http://www.lavasoft.de/default.shtml.es. A continuación: ejecutar Ad-Aware, clic en el botón con el engranaje para acceder a la configuración, clic en botón "Interface" (penúltimo de la lista de la izquierda) y en el desplegable junto a "Language File" seleccionar "spanish"; y clic en botón "Proceed" (abajo a la derecha de la ventana) para activar los cambios.

Spybot S&D: Programa gratuito, posibilidad de actualización por Internet. Sencillo y cómodo de utilizar. Cabe destacar la opción de dejarlo residente en memoria con lo cual recibimos aviso de todos las aplicaciones que intentan escribir en el registro de Windows. Tiene capacidad de eliminación de los spywares encontrados así como de evitar el secuestro del navegador; para lo cual hay que activar la opción de "Modo Avanzado" dirigirse a la pestaña de "Herramientas" y marcar "Páginas del navegador". Válido en todos los Sistemas Operativos Windows a partir del 98.

- **En inglés**

 CWShredder de Intermute: Programa gratuito especializado en la eliminación de todas las variantes del código espía CoolWebSearch que se pueden instalar en nuestro ordenador ocasionando distintos tipos de desastres dependiendo de su versión. Fácil de utilizar, sólo hay que tener el navegador cerrado en el momento del análisis. Válido para todos los Sistemas Operativos Windows.

 Hijackthis: Programa gratuito con posibilidad de actualización por Internet. Genera un informe con información referente a ciertos elementos del registro de Windows, ficheros y programas que se inician en el arranque del sistema; no todos ellos son espías ni código malicioso, así que hay que tener cuidado con lo que se selecciona para eliminar y preferiblemente consultar previamente a alguien con experiencia; también aconsejamos hacer una copia de seguridad para poder recuperar los cambios realizados. Válido para todos los Sistemas Operativos Windows.

 eTrust PestPatrol Anti-Spyware: Anti–*spyware* comercial. En su versión gratuita permite realizar un escaneo en línea mediante la descarga de un control ActiveX. Una vez realizado el análisis muestra un listado con todos los espías detectados en el equipo; no permite la eliminación automática de los mismos, pero pulsando sobre cualquiera de ellos, aparece una nueva ventana del navegador con información relativa a dicho espía y cómo eliminarlo manualmente. Válido para todos los sistemas operativos Windows.

 SpywareBlaster: Programa que previene la intrusión de Software maligno como espías, *adware*, *dialers*... en nuestro sistema, tanto de los que se intentan instalar mediante controles Active-X como por otros medios. Funciona para IExplorer y para MozillaFirefox. No realiza ni escaneo ni eliminación del software maligno que pudiera haber en el equipo, sólo funciona como un programa de prevención que impide la instalación de este software maligno en el ordenador. Hay que bajarse el programa y habilitar las opciones de prevención para que funcione correctamente. Permite crear una copia de seguridad de ciertas partes de nuestro equipo. Válido para todas las versiones de Windows.

 SpywareGuard: Permite escaneo en tiempo real evitando que el software espía llegue a ejecutarse y también tiene una protección antiespías durante las descargas de Internet, además evita los posibles secuestros del navegador IExplorer si se activa la opción de "Browser Hijack Protection". Crea un fichero de log en el que se pueden ver todas las acciones realizadas. Es fácilmente actualizable. Válido para todos los Sistema Operativos Windows.

 SpySweeper: Anti – *spyware* comercial. La versión demo no admite la actualización por Internet. Posee algunas herramientas interesantes de escudo activo, como la detección de entradas de *cookies* o *spywares* que sean un riesgo para nuestro sistema o evitar cambios no autorizados en la página de inicio del Internet Explorer, opción que viene activada por defecto y que se encuentra en la pestaña de "Shields", la sección de Internet Explorer en la opción "IEhome Page Shield". Tiene capacidad de eliminación de los espías encontrados. Válido en todos los Sistemas Operativos Windows a partir del 98.

4.3.5 Los 5 principales síntomas de infección son:

- Cambio de la página de inicio, la de error y búsqueda del navegador.
- Aparición de ventanas pop-ups, incluso sin estar conectados y sin tener el navegador abierto, la mayoría de temas pornográficos.
- Barras de búsquedas de sitios como la de Alexa, Hotbar, etc... que no se pueden eliminar.
- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.
- La navegación por la red se hace cada día más lenta.

4.4 Adware

El **adware** es software que durante su funcionamiento despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla. Esta práctica se utiliza para subvencionar económicamente la aplicación, permitiendo que el usuario la obtenga por un precio más bajo e incluso gratis y, por supuesto, puede proporcionar al programador un beneficio, que ayuda a motivarlo para escribir, mantener y actualizar un programa valioso.

Algunos programas adware son también shareware, y en estos los usuarios tiene la opción de pagar por una versión registrada o con licencia, que normalmente elimina los anuncios. Los programas adware han sido criticados porque ocasionalmente incluyen código que realiza un seguimiento de información personal del usuario y la pasa a terceras entidades, sin la autorización o el conocimiento del usuario. Esta práctica se conoce como spyware, y ha provocado críticas de los expertos de seguridad y los defensores de la privacidad, incluyendo el Electronic Privacy Information Center. Otros programas adware no realizan este seguimiento de información personal del usuario.

Existen programas destinados a ayudar al usuario en la búsqueda y modificación de programas adware, para bloquear la presentación de los anuncios o eliminar las partes de spyware. Para evitar una reacción negativa, como toda la industria publicitaria en general, los creadores de adware deben equilibrar sus intentos de generar ingresos con el deseo del usuario de no ser molestado.

4.5 Malware

La palabra **malware** proviene de una agrupación de las palabras **mal**icious soft**ware**. Este programa o archivo, que es dañino para el ordenador, está diseñado para insertar virus, gusanos, troyanos o spyware intentando conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí.

Dos tipos comunes de malware son los **virus** y los **gusanos** informáticos, este tipo de programas tienen en común la capacidad para auto replicarse, es decir, pueden contaminar con copias de sí mismo que en algunas ocasiones ya han mutado, la diferencia entre un gusano y un virus informático radica en que el gusano opera de forma más o menos

independiente a otros archivos, mientras que el virus depende de un portador para poderse replicar.

- **Los virus informáticos** utilizan una variedad de portadores. Los blancos comunes son los archivos ejecutables que son parte de las aplicaciones, los documentos que contienen macros, y los sectores de arranque de los discos de 3,1/2 pulgadas. En el caso de los archivos ejecutables, la rutina de infección se produce cuando el código infectado es ejecutado, ejecutando al mismo tiempo el código del virus. Normalmente la aplicación infectada funciona normalmente. Algunos virus sobrescriben otros programas con copias de ellos mismos, el contagio entre computadoras se efectúa cuando el software o el documento infectado van de una computadora a otra y es ejecutado.

- **Los gusanos** informáticos son similares a los virus, pero los gusanos no dependen de archivos portadores para poder contaminar otros sistemas. Estos pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema. Para contaminar otros sistemas, los gusanos explotan vulnerabilidades del objetivo o utilizan algún tipo de ingeniería social para engañar a los usuarios y poderse ejecutar.

- Un **programa caballo de troya** es una pieza de software dañino disfrazado de software legítimo. Los caballos de troya no son capaces de replicarse por si mismos y pueden ser adjuntados con cualquier tipo de software por un programador o puede contaminar a los equipos por medio del engaño.

- **Una puerta trasera**(o bien Backdoor) es un software que permite el acceso al sistema de la computadora ignorando los procedimientos normales de autenticación. De acuerdo en como trabajan e infectan a otros equipos, existen dos tipos de puertas traseras. El primer grupo se asemeja a los caballos de troya, es decir, son manualmente insertados dentro de algún otro software, ejecutados por el software contaminado e infecta al sistema para poder ser instalado permanentemente. El segundo grupo funciona de manera parecida a un gusano informático, el cuál es ejecutado como un procedimiento de inicialización del sistema y normalmente infecta por medio de gusanos que lo llevan como carga.

- **El spyware** es todo aquel software que recolecta y envía información de los usuarios. Normalmente trabajan y contaminan sistemas como lo hacen los caballos de troya.

- **Un exploit** es aquel software que ataca una vulnerabilidad particular de un sistema operativo. Los exploits no son necesariamente maliciosos –son generalmente creados por investigadores de seguridad informática para demostrar que existe una vulnerabilidad. Y por esto son componentes comunes de los programas maliciosos como los gusanos informáticos.

- **Los rootkit**, son programas que son insertados en una computadora después de que algún atacante ha ganado el control de un sistema. Los rootkit generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los log de entradas o encubrir los procesos del atacante. Los rootkit pueden incluir puertas traseras, permitiendo al atacante obtener de nuevo acceso al sistema o también pueden incluir exploits para atacar otros sistemas.

CAPITULO 5
MANTENIMIENTO PREVENTIVO Y CORRECTIVO PARA PC's DE LA DGTVE

5.1 Introducción

La computadora hoy en día se ha vuelto una herramienta indispensable en muchas áreas, lo mismo puede servir para calcular la distancia de la estrella más lejana de nuestro sistema solar como para la diversión y esparcimiento de un niño que la utiliza para jugar, al igual que el ama de casa la puede utilizar para llevar una gran colección de recetas de cocina, y como cualquier herramienta necesita cuidados y tratos especiales.

El medio ambiente que rodea a la computadora personal encuentra en ella un imán de polvo, se preguntará y esto en qué me afecta. Pues resulta que el polvo, aunado a un ambiente húmedo o muy seco puede ser un magnífico conductor eléctrico, lo cual puede provocar pequeñas fallas en los componentes electrónicos de la computadora personal, asimismo el polvo acumulado reduce la eficiencia de los ventiladores de enfriamiento y puede actuar como un manto aislante que conserva el calor y no permite que la irradiación de éste se aleje de los componentes. De este modo, se debe limpiar el sistema tomando en cuenta que dependiendo del medio ambiente que rodee la computadora dependerá la periodicidad con que se lleve a cabo esta tarea.

5.2 ¿Qué es el mantenimiento para PC's?

Es el cuidado que se le da a la computadora para prevenir posibles fallas, se debe tener en cuenta la ubicación física del equipo ya sea en la oficina o en el hogar, así como los cuidados especiales cuando no se está usando el equipo. Hay dos tipos de mantenimiento, el preventivo y el correctivo.

5.3 Tipos de mantenimiento para la PC

- ***Mantenimiento preventivo para PC's***

El mantenimiento preventivo consiste en crear un ambiente favorable para el sistema y conservar limpias todas las partes que componen una computadora. El mayor número de fallas que presentan los equipos es por la acumulación de polvo en los componentes internos, ya que éste actúa como aislante térmico. El calor generado por los componentes no puede dispersarse adecuadamente porque es atrapado en la capa de polvo.

Las partículas de grasa y aceite que pueda contener el aire del ambiente se mezclan con el polvo, creando una espesa capa aislante que refleja el calor hacia los demás componentes, con lo cual se reduce la vida útil del sistema en general. Por otro lado, el polvo contiene elementos conductores que pueden generar cortocircuitos entre las trayectorias de los circuitos impresos y tarjetas de periféricos. Si se quiere prolongar la vida útil del equipo y hacer que permanezca libre de reparaciones por muchos años se debe de realizar la limpieza con frecuencia.

- ***Mantenimiento correctivo para PC's***

Consiste en la reparación de alguno de los componentes de la computadora, puede ser una soldadura pequeña, el cambio total de una tarjeta (sonido, video, SIMMS de memoria, entre otras), o el cambio total de algún dispositivo periférico como el ratón, teclado, monitor, etc.

Resulta mucho más barato cambiar algún dispositivo que el tratar de repararlo pues muchas veces nos vemos limitados de tiempo y con sobre carga de trabajo, además de que se necesitan aparatos especiales para probar algunos dispositivos.

Asimismo, para realizar el mantenimiento debe considerarse lo siguiente:

- En el ámbito operativo, la reconfiguración de la computadora y los principales programas que utiliza.
- Revisión de los recursos del sistema, memoria, procesador y disco duro.
- Optimización de la velocidad de desempeño de la computadora.
- Revisión de la instalación eléctrica (sólo para especialistas).
- Un completo reporte del mantenimiento realizado a cada equipo.
- Observaciones que puedan mejorar el ambiente de funcionamiento.

5.4 Criterios que se deben considerar para el mantenimiento a la PC

La periodicidad que se recomienda para darle mantenimiento a la PC es de una vez por semestre, esto quiere decir que como mínimo debe dársele dos veces al año, pero eso dependerá de cada usuario, de la ubicación y uso de la computadora, así como de los cuidados adicionales que se le dan a la PC.

Por su parte, la ubicación física de la computadora en el hogar u oficina afectará o beneficiará a la PC, por lo que deben tenerse en cuenta varios factores:

- ***Hogar***

Es necesario mantener el equipo lejos de las ventanas, esto es para evitar que los rayos del sol dañen a la PC, así como para evitar que el polvo se acumule con mayor rapidez, también hay que tratar de ubicar a la PC en un mueble que se pueda limpiar con facilidad, si en la habitación donde se encuentra la PC hay alfombra se debe aspirar con frecuencia para evitar que se acumule el polvo. También no es conveniente utilizar el monitor como "repisa", esto quiere decir que no hay que poner nada sobre el monitor ya que genera una gran cantidad de calor y es necesario disiparlo, lo mismo para el chasis del CPU.

- ***Oficina***

Los mismos cuidados se deben tener en la oficina, aunque probablemente usted trabaje en una compañía constructora y lleve los registros de materiales, la contabilidad, los planos en Autocad, etc. Esto implicaría que la computadora se encuentre expuesta a una gran cantidad de polvo, vibraciones y probablemente descargas eléctricas, así mismo la oficina se mueve a cada instante, hoy puede estar en la Ciudad de México y en dos semanas en Monterrey, por lo mismo el mantenimiento preventivo será más frecuente.

Consideraciones finales:

- No exponer a la PC a los rayos del sol.
- No colocar a la PC en lugares húmedos.
- Mantener a la PC alejada de equipos electrónicos o bocinas que produzcan campos magnéticos ya que pueden dañar la información.
- Limpiar con frecuencia el mueble donde se encuentra la PC así como aspirar con frecuencia el área si es que hay alfombras.
- No fumar cerca de la PC.
- Evitar comer y beber cuando se esté usando la PC.
- Usar “No-Break” para regular la energía eléctrica y por si la energía se corta que haya tiempo de guardar la información.
- Cuando se deje de usar la PC, esperar a que se enfríe el monitor y ponerle una funda protectora, así como al teclado y al chasis del CPU.
- Revisión de la instalación eléctrica de la casa u oficina, pero esto lo debe de hacer un especialista.

5.5 Material, herramientas y mesa de trabajo

Como ya se había explicado anteriormente el mantenimiento preventivo ayudará a alargar el buen funcionamiento de la PC, para ello se tiene que contar con una mesa de trabajo, la cual preferentemente no debe de ser conductora (que no sea de metal o similar), se debe de tener el área o mesa de trabajo libre de estorbos y polvo.

Ahora bien, si ya se está dispuesto a dar mantenimiento a la computadora, será conveniente establecer medidas de seguridad y más o menos determinar cuál será el área de trabajo ideal para abrir la computadora. La mayor de las veces que uno realiza un trabajo, cualquiera que sea éste, es necesario siempre contar con todo el material, herramientas y área de trabajo adecuados para llevar a buen término dicha tarea. Un ejemplo muy simple es el siguiente: si al retirar una tuerca para remover una pieza mecánica, no cuento con una llave adecuada, y por falta de tiempo utilizo unas pinzas de presión, de momento se soluciona el problema, pero al no utilizar la llave adecuada se pueden ocasionar problemas que van desde el maltrato de la tuerca en el menor de los casos, y en el peor su deformación por la aplicación excesiva de presión, con la consecuencia de quedar inutilizada y tener que retardar el término de la tarea.

El ejemplo anterior muestra de una manera muy simple el problema que se puede ocasionar sino no se cuenta con la herramienta adecuada. En el caso de equipo de cómputo el uso inadecuado de herramientas puede causar conflictos muy sencillos como cambiar un tornillo, y tan graves como cambiar una tarjeta electrónica (Madre, video, sonido, etcétera). La mesa de trabajo es una parte importante para poder realizar eficientemente el trabajo de limpieza así como su amplitud es una característica importante, ya que es necesario contar con el espacio adecuado para no correr el riesgo de que se caigan los componentes retirados del gabinete (cables, tarjetas de expansión, etcétera).

Una iluminación adecuada es indispensable para poder observar las áreas que se limpiarán, a la par de una mejor identificación de los componentes de la computadora para evitar confusiones al momento de conectar los diferentes cables que hay dentro del sistema.

En el mercado hay diferentes tipos de destornilladores, debido al diseño de la punta que tienen: plano, de cruz, estrella y de caja.

De todos los tipos de destornilladores mencionados se necesitarán, por lo menos un juego de tres medidas en cada uno de los casos, en cuanto a los destornilladores de caja si conviene tener un juego completo.

Las pinzas son una herramienta sumamente útil ya que ayudan a llegar a esos rincones donde a veces no entran sus dedos y es necesario tomar o conectar algo de ahí. También sirven para enderezar los contactos que a veces por las prisas doblamos.

Hay varios tipos de pinzas, de las cuales ocupará sólo las de punta y corte, ambas por lo menos en dos tamaños, pequeñas y medianas.

Muchos de los circuitos del interior de la computadora son susceptibles de sufrir daños a causa de la electricidad estática. Una simple descarga puede inutilizar los circuitos integrados, lo cual a su vez puede repercutir en un mal y hasta inhabilitar el equipo. Debido a que la electricidad estática puede inclusive generarse en el cuerpo humano —esto variará dependiendo de cada uno como individuo— se necesitan tomar unas cuantas precauciones cuando se estén manejando componentes de la computadora, y una de ellas es ocupar la pulsera antiestática.

La pulsera antiestática es un dispositivo que se adapta a su muñeca y lo conecta a una fuente de tierra (como la parte metálica de una caja) para mantenerlo libre de electricidad estática. Si tiene alfombra en el cuarto donde está trabajando con la computadora, tome sus precauciones contra la descarga de electricidad estática que definitivamente se generará en su cuerpo. En cualquier caso, no arrastre demasiado los pies mientras se encuentre trabajando con la computadora. Se generará menos electricidad estática de esta manera.

Una vez que se han tomado las anteriores recomendaciones, hay que comenzar a darle mantenimiento al CPU y sus componentes. **No hay que olvidar apagar la computadora y desconectar el cable de alimentación de la toma de energía.**

5.5.1 Tarjeta Madre

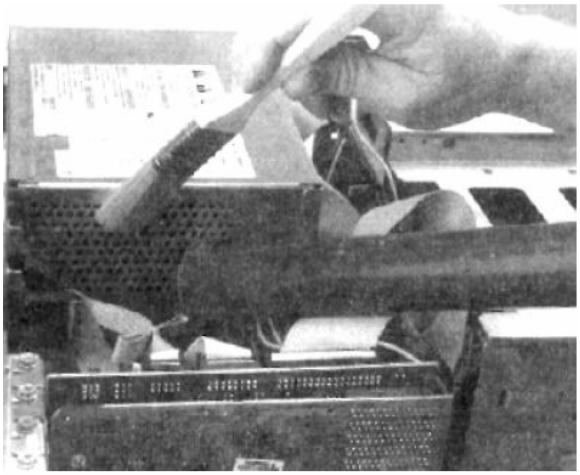
Las mejores herramientas para esta labor son una brocha de cerdas rígidas limpia, una aspiradora y un producto limpiador-desengrasante. Utilice la brocha para remover el polvo adherido a los componentes para que la aspiradora pueda a su vez quitarlo. Aunque se debe de aspirar todo el polvo que se encuentre dentro del sistema hasta donde sea posible (sin exagerar al remover puentes, disipadores adheridos por pegamento o grapas, etc.), hay que poner especial énfasis en las siguientes áreas:

- **Ventilador del CPU**. Éste puede acumular casi tanto polvo como la fuente de poder, y como el CPU genera demasiado calor, es importante conservar limpio el ventilador para mantener en buen estado su capacidad de enfriamiento. Por lo tanto, si a simple vista se nota que éste ha sufrido deterioro por el paso del tiempo, o usted a notado que produce un ruido excesivo, será necesario que lo cambie, ya que el calentamiento excesivo en el CPU puede provocar fallos del sistema.

- **Ranuras de expansión (ISA, PCI y AGP).** Al mantener el polvo fuera de estas ranuras se asegura una buena calidad de conexión, si se instala posteriormente una tarjeta adaptadora en la ranura.

Una vez retirado el polvo excesivo se puede aplicar un producto que acabe de retirar la suciedad de la tarjeta y que normalmente contiene una sustancia desengrasante; esto sirve para evitar que pequeños residuos de grasa provoquen la acumulación temprana de polvo.

PRECAUCIÓN. *Se deberá resistir la tentación de invertir el flujo del aire de la aspiradora o emplear aire comprimido para soplar el polvo fuera de la computadora. En primer lugar, sólo se lograría soplar el polvo de regreso a la habitación, de manera que puede caer otra vez dentro de la computadora. Sin embargo es más importante el hecho de que el polvo tiene la tendencia a abrirse paso dentro de las unidades lectoras de disco flexible, ranuras de expansión y otros lugares difíciles de alcanzar. Además, cuide que la brocha y la boquilla de la aspiradora no golpeen ni dañen algo.*



Limpiando la fuente de poder.

5.5.2 SIMMs y DIMMs de memoria RAM

Para poder limpiar los SIMMs y DIMMs es necesario desmontarlos de la Tarjeta madre, a continuación se explica cómo hacerlo.

Extraer un SIMM no es una tarea muy difícil, para extraerlos de la ranura, basta con presionar las lengüetas laterales. Si no es posible hacerlo con los dedos, puede hacerse con la ayuda de un destornillador plano, teniendo mucho cuidado de no dañar ningún componente. En especial hay que evitar clavar el destornillador o rayar con él la superficie de la tarjeta madre. El procedimiento para retirar el polvo de estos dispositivos es exactamente igual al estudiado con anterioridad (Tarjeta Madre), sólo habrá que añadir que en caso de que las terminales se encuentren sucias se recomienda limpiarlas con una goma de lápiz, asegurándose de que no sea demasiado dura para no maltratar las terminales. Acto seguido se podrá aplicar sobre los mismos el producto desengrasante para eliminar cualquier residuo de grasa que pudiera existir.

Se debe tener cuidado de tomar por los bordes los SIMMs y DIMMs para evitar posibles daños por descarga de electricidad estática generada por nuestro cuerpo. Es

importante recalcar lo anterior ya que a veces estos dispositivos no se dañan de inmediato, pero se van degradando poco a poco, reduciendo así la vida útil de éstos.

Una vez acabado el proceso de limpieza, hay que volver a colocar los SIMMs, lo cual implica un proceso donde habrá que observar que éstos tienen una pequeña muesca en uno de los lados y en la base de la ranura donde se inserta, hay una pequeña rebaba de plástico que permite insertar el modulo de la memoria únicamente cuando coincide con esta rebaba. Si esta operación se realiza correctamente, se empuja el módulo de memoria hasta que las lengüetas hacen un pequeño chasquido cuando se sitúan en su posición y aseguran el módulo de memoria.

5.5.3 Unidades lectoras y de almacenamiento

- **Disco duro**

Por lo regular, no hay nada que hacer para limpiar un disco duro, de hecho, si se llegara a abrir un disco duro, en ese momento se haría inmediatamente inservible, ya que la mínima partícula de polvo o del medio ambiente, pueden destruir la cabeza de un disco duro. Por tanto, la limpieza del disco duro, solamente implica retirar el polvo depositado sobre la superficie externa con una brocha y aspiradora.

- **Unidad lectora de disco flexible**

Otro dispositivo que se debe de limpiar cada cierto tiempo es la unidad lectora de disco flexible de la computadora. A diferencia de las cabezas de un disco duro, que se desplazan sobre el disco en un cojín de aire, las de una unidad lectora de disco flexible descansan sobre la superficie del medio magnético del disco flexible. De este modo, la cabeza tiene la tendencia a acumular en forma progresiva la suciedad del disco. Si las cabezas llegan a ensuciarse en demasía, la unidad no podrá leer ni escribir en el disco.

La limpieza de la unidad lectora no requiere que se desarme nada. En vez de ello, requiere de un limpiador especial, que se puede adquirir en cualquier tienda de productos de computación.

El disco limpiador tiene el aspecto de un disco normal, sólo que la parte interior de la cubierta del disco está hecha de una tela suave y porosa en lugar del substrato plástico/magnético empleado en un disco normal. El conjunto de limpieza incluye un líquido que se aplica en la tela del disco. Posteriormente se introduce este disco en la unidad lectora y se intentará tener acceso a él, mediante el comando **DIR A:** si está en ambiente de DOS, o presionar dos veces el botón izquierdo del ratón en la unidad A: de la ventana de Mi PC, en Windows 95, 98 y Windows NT 4.0.

5.5.4 Fuente de alimentación

Nunca abra la fuente de poder para tratar de limpiar el interior, aunque se puede y debe aspirar el polvo de los orificios laterales de la fuente. Esto ayuda al buen funcionamiento del ventilador de la misma y lo capacita para sacar más aire del gabinete. Además en la parte posterior de la fuente de poder, se puede aspirar el polvo acumulado sobre la superficie de las aspas del ventilador. Tal vez sea posible retirar temporalmente la

protección de alambre que lo cubre (si es movible), para poder tener acceso a las aspas y remover el polvo con la brocha de cerdas firmes y finalizar con la aspiradora, pero asegúrese de volver a colocar la protección cuando haya acabado la limpieza.

5.5.5 Tarjetas en el sistema

Para poder realizar la limpieza de estos dispositivos será necesario desmontarlos de las ranuras de expansión, lo cual sólo implica retirar un tornillo que fija la tarjeta a la estructura del gabinete y evita que se desprenda.

El procedimiento para retirar el polvo de estos dispositivos es exactamente igual al estudiado con anterioridad (Tarjeta Madre), sólo debe añadirse que en caso de que las terminales se encuentren sucias se recomienda limpiarlas con una goma de lápiz, asegurándose de que no sea demasiado dura para no maltratar las terminales. Acto seguido se podrá aplicar sobre los mismos el producto desengrasante para eliminar cualquier residuo de grasa que pudiera existir.

Se debe tener cuidado de tomar por los bordes laterales las tarjetas para evitar posibles daños por descarga de electricidad estática generada por nuestro cuerpo. Es importante recalcar lo anterior ya que a veces estos dispositivos no se dañan de inmediato, pero se van degradando poco a poco, reduciendo así la vida útil de éstos.

El proceso de montaje de las tarjetas, al igual que el desmontaje no representa mayor problema más que introducir la tarjeta a su ranura, la mayor dificultad consistiría en que entrara muy ajustada, pero incorporando primero una de las esquinas y después el resto de la tarjeta en la ranura se soluciona el problema. **Asegúrese de que inserta la tarjeta en la ranura adecuada.**

5.6 Mantenimiento preventivo a dispositivos

Antes que nada habrá que definir que los dispositivos a los cuales les daremos mantenimiento son considerados periféricos. Estos pueden ser de entrada, de salida y también los hay de entrada y salida. De los dispositivos periféricos a los cuales se les dará mantenimiento y se explica a continuación, los podemos considerar como: de salida al monitor y de entrada al teclado y ratón.

Un dispositivo de entrada es aquél que mandará información al CPU. Un dispositivo de salida será aquél que reciba información del CPU. Por lo tanto, un dispositivo de entrada y salida será con el que se pueda enviar y recibir información del CPU.

Aunque en este documento no se explicará cómo dar mantenimiento a todos los dispositivos periféricos más utilizados, por lo menos es conveniente saber cuáles son: impresoras, módems, cámaras digitales, micrófonos, escáner (digitalizador de imágenes), y las unidades de CD-ROM externas.

5.6.1 Monitor

En ningún momento cuando se habla de mantenimiento preventivo, se debe de pensar en que se va a abrir el monitor para limpiarlo. El monitor contiene condensadores de alta capacidad eléctrica que pueden producir un peligroso y hasta mortal choque eléctrico incluso después de haberlo apagado y desconectado. De cualquier modo, no hay mucho que se pueda limpiar en el interior del monitor.

En vez de ello, hay que concentrarse en limpiar el exterior del monitor y la pantalla. Generalmente se ocupa una buena solución limpiadora de cristales para limpiar, no solamente el vidrio de la pantalla, sino también el gabinete. Hay que ocupar un lienzo libre de pelusa y vaciar el limpiador sobre el lienzo, no sobre el cristal. Esto evitará que el fluido escurra y se introduzca en el espacio entre el cristal y el gabinete. Lo anterior es muy importante recalcarlo ya que no se debe de introducir el fluido al interior del gabinete, porque podría provocar un corto circuito en el monitor.

5.6.2 Teclado

Es sorprendente la cantidad de suciedad y basura que se puede llegar a acumular en un teclado. La primera línea de defensa es un bote con gas comprimido (vea la figura), que se puede encontrar en tiendas de productos de computación y electrónica. La lata incluye un diminuto popote o pajilla para su aplicación, que se ajusta en la boquilla de la lata y le permite dirigir el gas a sitios de difícil acceso, como los espacios entre las teclas.

Aplicación de aire comprimido al teclado para limpieza externa.

Esta operación de soplado del teclado se debe de realizar en un lugar aparte del sitio donde generalmente trabaja con su computadora, y para evitar que eventualmente este polvo y suciedad regrese, utilice la aspiradora para juntar la basura a medida que ésta sea expedida por el aire comprimido.

Aunque normalmente no se necesita desarmar el teclado para limpiar el polvo y los desechos que caen sobre el mismo, tal vez se necesite desarmar para limpiar alguna cosa que se haya derramado en él. El agua no afectará sino se derrama en demasía. Si sólo fueron unas cuantas gotas, no importa, se evaporarán por sí solas. Si se derrama refresco de

cola u alguna otra cosa que contenga azúcar, realmente se debe abrir el teclado y limpiarlo a fondo.

Antes de limpiar dentro del teclado necesitará:

- Un destornillador de cruz para desarmar el teclado.
- Gas comprimido y/o brocha y aspiradora.
- Alcohol isopropílico para limpiar y un lienzo libre de pelusas.

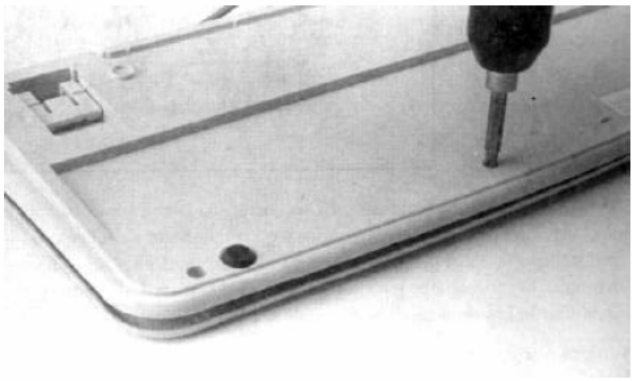
El siguiente procedimiento sirve para limpiar a fondo el teclado.

1. Cierre el sistema y apague su computadora.

2. Desconecte el teclado de la computadora y colóquelo de cabeza sobre una superficie de trabajo limpia y plana.

NOTA. *Si planea desarmar el teclado y quitar las teclas para limpiar debajo de ellas, es una buena idea hacer una fotocopia de la distribución del teclado. Puede utilizar posteriormente esta fotocopia para asegurarse de que tenga todas las teclas de vuelta en su posición correcta.*

3. Retire los tornillos que mantienen unida la cubierta del teclado (vea figura).



Cómo retirar los tornillos que fijan la cubierta del teclado.

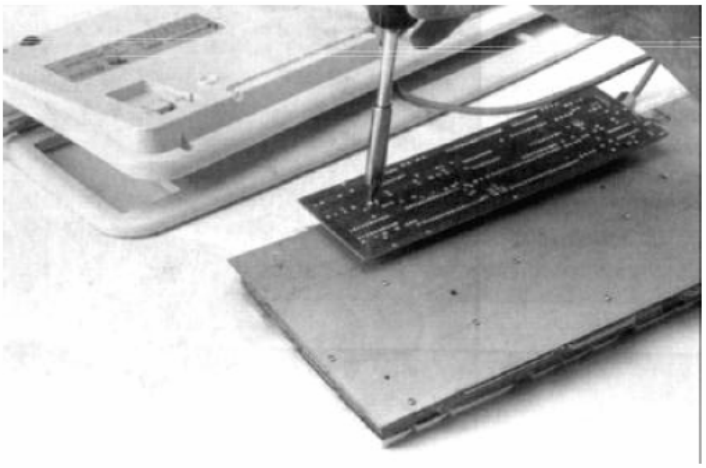
4. Manteniendo unida la cubierta, dé vuelta al teclado, y retire la cubierta superior. Emplee el gas comprimido y/o brocha y la aspiradora para limpiar las teclas (vea la figura).

Aplicando aire comprimido a las teclas para una limpieza profunda.

NOTA. Si sólo quiere limpiar el polvo y suciedad diversa del teclado, deténgase aquí y vuelva a ensamblar el teclado, los pasos siguientes son para la limpieza de derrames.

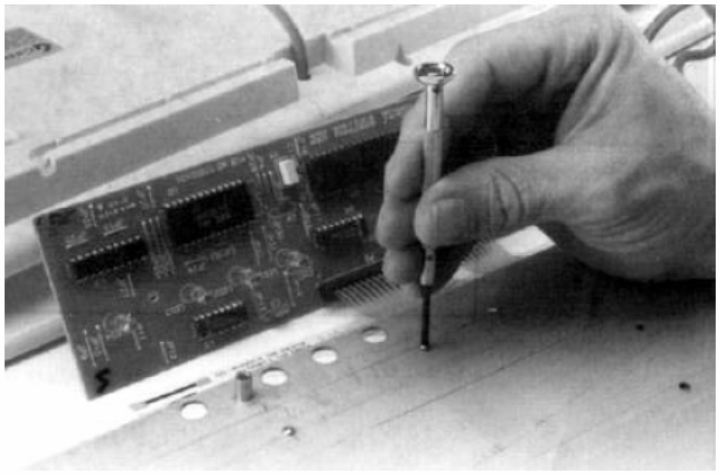
5. Teniendo cuidado de que no se caiga ninguna tecla, quite el dispositivo de las teclas del gabinete.

6. Si el teclado tiene una tarjeta de circuitos unida al dispositivo de las teclas (ver figura), retírela y hágala a un lado (observe la manera en que está conectada dicha tarjeta).



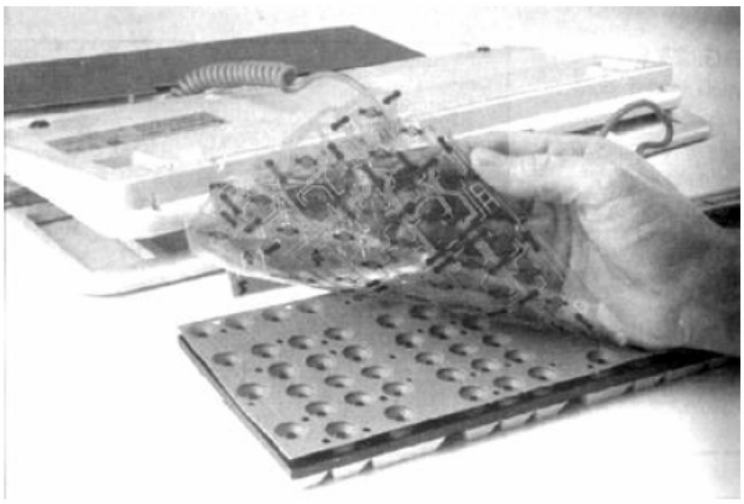
Cómo retirar la tarjeta de circuitos de la base del teclado.

7. Retire los tornillos que sostienen la placa metálica en la parte posterior del dispositivo del teclado. Ponga los tornillos en una taza u otro recipiente, de manera que no se pierdan, (ver figura).



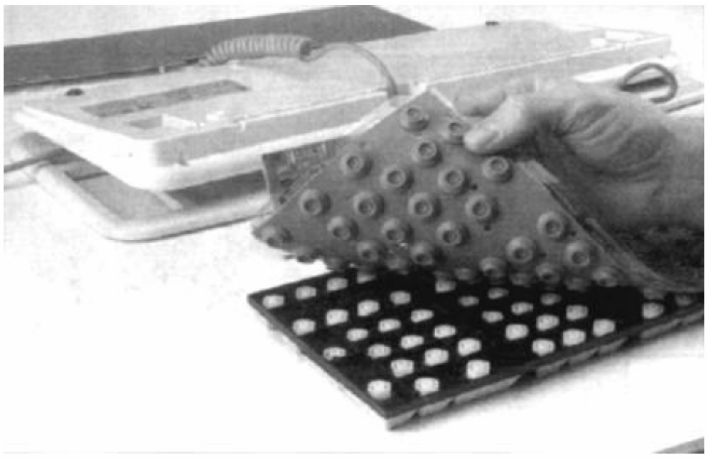
Retirando los tornillos de la placa metálica.

8. Levante cuidadosamente la placa de metal. Lo que encontrará debajo de ella depende del diseño del teclado; la figura siguiente es una muestra bastante típica de lo que verá: alguna clase de circuito impreso. Con sumo cuidado levante y limpie los contactos de la tarjeta con el alcohol y el lienzo.



Retirando el circuito impreso para limpieza.

9. Probablemente, habrá un tipo de almohadilla de hule entre el circuito impreso y la parte posterior de las teclas (ver figura siguiente). Levante cuidadosamente ésta y limpie cualquier residuo de derrames de dicha almohadilla, así como de la parte posterior de las teclas.

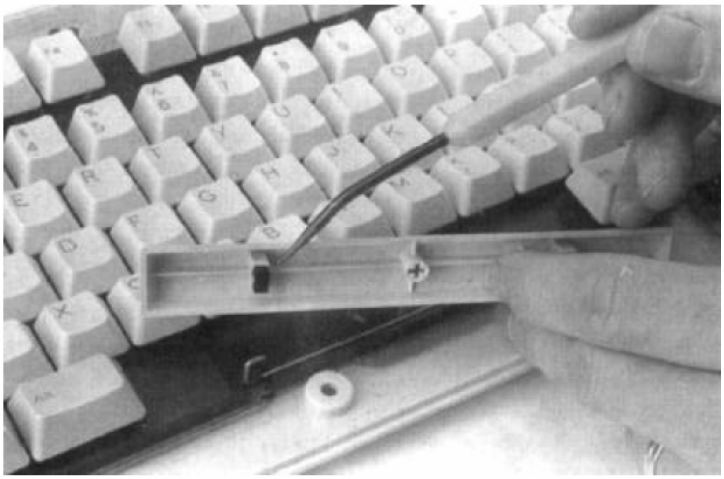


Limpieza de almohadilla (membrana).

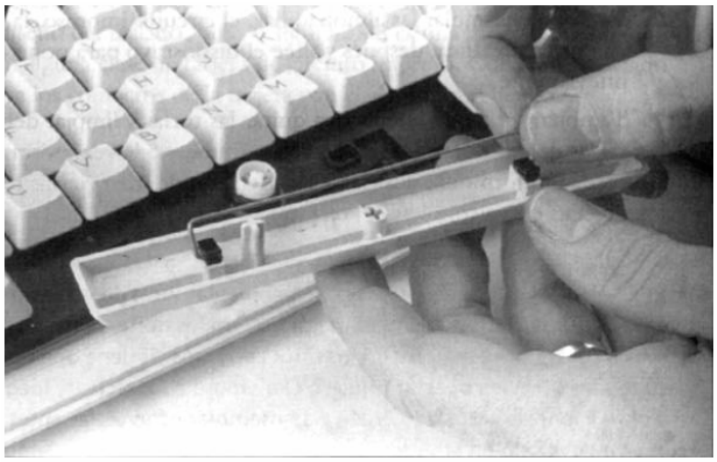
10. Vuelva a ensamblar las almohadillas, el circuito impreso, la tarjeta del circuito y la placa metálica, después voltee el dispositivo para ponerlo al derecho nuevamente.

11. También sería una buena idea quitar las teclas y limpiar debajo de ellas. Las teclas deben botarse, pero no retire muchas a la vez, porque tendrá un gran problema tratando de deducir donde irían ciertas teclas. Limpie debajo de ellas con alcohol y un lienzo.

PRECAUCIÓN. *Algunas de las teclas tienen alambres de retención debajo de ellas (véanse figuras siguientes). Es mejor que no los quite, porque puede ser difícil volver a colocar los alambres en los sitios correctos. Si tiene que quitarlos, tal vez le resulte más sencillo conectar primero el alambre a las teclas, y luego conectar el alambre y la tecla al teclado. Vuelva a ensamblar estas teclas antes de que coloque la cubierta de nuevo en el teclado, para facilitar el acceso a los alambres y conectores.*



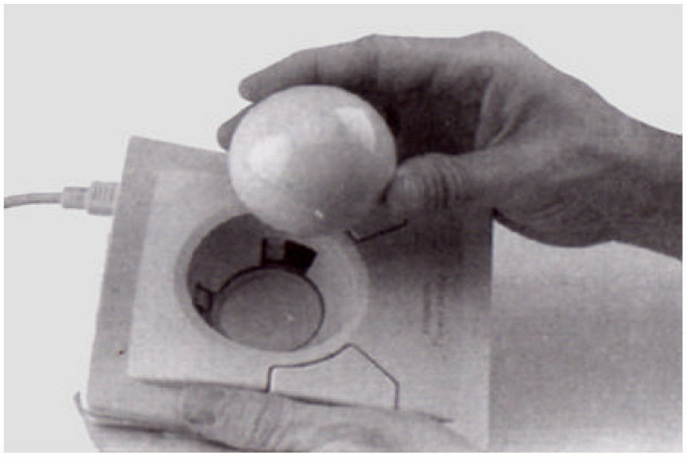
Identificación de soportes de los alambres de retención.



Cómo colocar el alambre de retención.

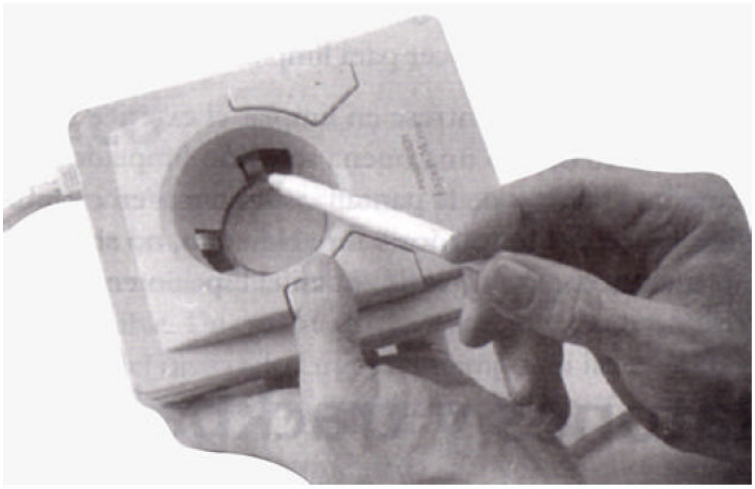
5.6.3 Ratón

Es buena idea limpiar ocasionalmente el interior de su ratón, ya sea normal, o de tipo estacionario. Hay dos clases principales: ópticos y mecánicos. Los dispositivos mecánicos tiene una esfera sin características especiales que moviliza pequeños rodillos a medida que se desplaza el ratón en una superficie, en la figura se muestra la esfera retirada de un ratón.



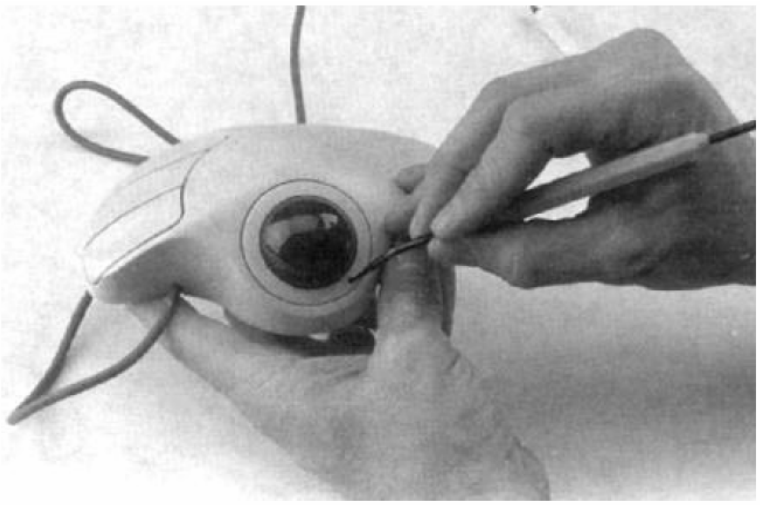
Esfera del ratón.

En la siguiente figura se ilustran los rodillos que se encuentran debajo de ella. El movimiento de los rodillos se traduce en una señal eléctrica que pasa a la PC. Con el tiempo, se va acumulando la suciedad en los rodillos y provoca problemas en el movimiento de la esfera. Se puede utilizar un lienzo de algodón o un paño humedecido de alcohol para limpiar los rodillos; o simplemente raspe la materia acumulada con la uña de su dedo. Asegúrese de quitar la basura del dispositivo antes de que vuelva a colocar la esfera en su lugar.



Rodillos del ratón.

Los ratones tienen un anillo de retención que mantiene a la esfera en su lugar, (ver figura). Para quitar la esfera, se debe de girar el anillo en dirección contraria a la de las manecillas del reloj y sacar el anillo. Luego se podrá quitar la esfera.



Cómo retirar el anillo de retención de la esfera.

5.7 Mantenimiento al Sistema Operativo

En estos momentos, dada la valía de la información que guardan, la seguridad de nuestros equipos informáticos es sencillamente imprescindible. Cada vez resulta más habitual vernos invadidos por virus informáticos, mensajes de publicidad emergentes, troyanos e incluso robos de información personales de la más diversa índole. Por todo ello, tan pronto como contemos con una conexión a Internet y utilicemos nuestra máquina para las tareas que más se han popularizado en los últimos tiempos (descarga de ficheros de música y video, conversación en línea a través de algún servicio de chat, lectura de los mensajes llegados a las diferentes cuentas de correo electrónico, navegación web en páginas de ocio, etc.), hemos de observar ciertas precauciones y tener conocimiento de diversas técnicas que nos tengamos que enfrentar a cualquier problema de seguridad.

5.8 Actualizaciones al día

Lo más importante, por encima de todas las posibles medidas que podamos asumir para asegurar nuestra máquina, es contar con un sistema operativo perfectamente actualizado y puesto al día. La razón es que son innumerables los fallos de seguridad que se descubren mes a mes en un sistema como por ejemplo Windows XP. Y no se trata solamente de incidencias que afecten a la fiabilidad de la conexión de red o a puertos indebidamente abiertos, ya que esta clase de supuestos podrían ser correctamente cubiertos con un buen corta fuegos. Muchos de estos agujeros que menos importancia dan los usuarios y que más difícilmente puede controlar un programa de seguridad son los que afectan a los programas que usamos a diario.

Algunos, como por ejemplo el navegador o el cliente de correo electrónico, pueden convertir nuestra máquina en vulnerable si accedemos a una página inadecuada o recibimos un mensaje maligno. Y ante esta clase de ataques, muchos cortafuegos y suites especializadas apenas los identifican. Por ello, y por encima de todo, siempre hemos de contar con el último **Service Pack** del sistema operativo instalado y revisar periódicamente la página de **Windows Update (www.windowsupdate.com)** para mantener nuestro ordenador al día de la mejor manera posible. De hecho, si podemos tener la función de **Actualizaciones Automáticas** de nuestro equipo, que mejor, pues esta tarea se realizará de manera transparente y automática.

5.8.1 Uso de Windows Update

- **¿Qué es Windows Update?**

  Un sitio Web de Microsoft que ofrece actualizaciones para el software del sistema operativo Windows y el hardware basado en Windows. Las actualizaciones tratan problemas conocidos y mejoran la protección frente a amenazas de seguridad.

- **¿Cómo funciona?**
  Cuando visita el sitio Web, Windows Update explora el equipo e indica las actualizaciones que se aplican al software y al hardware. Deberá seleccionar las actualizaciones que desea instalar y cómo instalarlas.

- **¿Qué tipos de actualizaciones puedo conseguir?**
  Microsoft ofrece varios tipos de actualizaciones que tratan una amplia variedad de problemas. Para que le resulte más fácil escoger las actualizaciones más importantes, aquellas que mejoran la protección del equipo y de la información, Windows Update utiliza las siguientes categorías:

  a) Alta prioridad

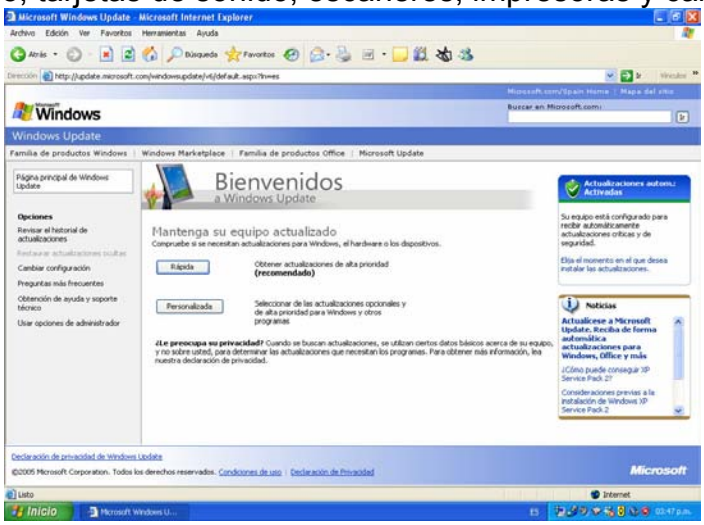
  Actualizaciones críticas, actualizaciones de seguridad, Service Packs y paquetes acumulativos de revisiones que debería instalar tan pronto como estén disponibles y antes de instalar otras actualizaciones.

  b) Software (opcional)

  Revisiones no críticas para programas de Windows, como el Reproductor de Windows Media® y el Visor de Windows Journal 1.5.

  c) Hardware (opcional)

  Revisiones no críticas para controladores y otros dispositivos de hardware, como tarjetas de vídeo, tarjetas de sonido, escáneres, impresoras y cámaras.



- **¿Qué diferencia hay entre la instalación rápida y la personalizada?**

  Rápida (recomendada) muestra todas las actualizaciones de alta prioridad para el equipo para que pueda instalarlas con un solo clic. Es la manera más rápida y sencilla de mantener el equipo actualizado.

  Personalizada muestra actualizaciones de alta prioridad y opcionales para el equipo. Debe revisar y seleccionar las actualizaciones que desea instalar, una a una.

- **¿Tengo que instalar las actualizaciones opcionales?**

  No. Las actualizaciones opcionales tratan problemas poco importantes o agregan al equipo funciones que no son críticas. Es más importante instalar las actualizaciones

de alta prioridad para que el equipo disponga del software crítico y relacionado con la seguridad más reciente.

- **¿Puedo conseguir actualizaciones automáticamente?**

  Sí, para ello debe activar Actualizaciones automáticas. Windows buscará las actualizaciones de alta prioridad más recientes para el equipo y las instalará según la configuración de Actualizaciones automáticas.

- **¿Es lo mismo Actualizaciones automáticas que Windows Update?**
  Sí, pero Actualizaciones automáticas sólo ofrece actualizaciones de alta prioridad. Para conseguir actualizaciones opcionales, debe visitar el sitio Web de Windows Update.

- **¿Qué es Actualizaciones automáticas?**
  Es una característica que funciona con Windows Update para ofrecer actualizaciones críticas y relacionadas con la seguridad a medida que están disponibles. Cuando se activa Actualizaciones automáticas (recomendado), Windows busca automáticamente las actualizaciones de alta prioridad para el equipo. El usuario decide cuándo y cómo se instalarán las actualizaciones.

- **¿Cómo puedo obtener más información sobre una actualización antes de instalarla?**
  Haga clic en el nombre de cada actualización para ver su descripción. Para ver los requisitos del sistema y la información de soporte técnico, haga clic en el vínculo **Detalles** que aparece en cada descripción.

- **¿Tengo que hacer algo para instalar una actualización?**
  En algunas ocasiones. Algunas actualizaciones requieren la aceptación de un Contrato de licencia para el usuario final (CLUF), responder a una pregunta sobre el proceso de instalación o reiniciar el equipo para poder instalarlas.

- **¿Qué ocurre si selecciono la opción "No volver a mostrar esta actualización"?**

  Windows Update ya no le pedirá que revise o instale dicha actualización. Sin embargo, si oculta una actualización de alta prioridad, puede que se le recuerde que falta una actualización que es crítica para la seguridad del equipo.

- **¿Con qué frecuencia se ofrecen nuevas actualizaciones en Windows Update?**
  Se ofrecen actualizaciones relacionadas con la seguridad una vez al mes. Sin embargo, si se produce una amenaza de seguridad, como un virus o un gusano extendido que afecta a los equipos basados en Windows, Microsoft ofrecerá la actualización correspondiente lo antes posible.
  Los demás tipos de actualizaciones se ofrecen cuando están disponibles. Puede ser útil activar Actualizaciones automáticas para que el equipo pueda recibir las actualizaciones de alta prioridad en cuanto estén disponibles.

- **¿Cómo puedo agregar Windows Update a mi lista de sitios Web de confianza?**
  No es necesario, ya que Internet Explorer cuenta con una forma de acceder a Windows Update directamente, en la opción Herramientas>esta Windows Update o desde Inicio>Programas> Windows Update.

- **¿Qué sistemas operativos admite Windows Update?**
  El sitio Web de Windows Update ofrece actualizaciones únicamente para sistemas operativos Windows.

Versión del sistema operativo	Soporte técnico de Windows Update
Windows Server 2003	
Windows Server 2003 con Service Pack 1	Se ofrecen actualizaciones
Windows Server 2003	No se ofrecerán nuevas actualizaciones a partir de junio de 2007
Windows XP	
Windows XP con Service Pack 2	Se ofrecen actualizaciones
Windows XP con Service Pack 1	No se ofrecen nuevas actualizaciones a partir de septiembre de 2006; las actualizaciones anteriores están disponibles
Windows XP	No se ofrecen nuevas actualizaciones a partir de septiembre de 2004; las actualizaciones anteriores están disponibles
Windows 2000	
Windows 2000 con Service Pack 4	Se ofrecen actualizaciones
Windows 2000 con Service Pack 3	No se ofrecen nuevas actualizaciones a partir de junio de 2005; las actualizaciones anteriores están disponibles
Windows 2000 con Service Pack 2	No se ofrecen nuevas actualizaciones a partir de junio de 2004; las actualizaciones anteriores están disponibles
Windows 2000 con Service Pack 1	No se ofrecen nuevas actualizaciones a partir de agosto de 2004; las actualizaciones anteriores están disponibles
Windows 2000	Ya no se admite
Otros sistemas operativos	
Windows Millennium Edition	Sólo se ofrecen actualizaciones críticas y de seguridad a partir de diciembre de 2003; no se ofrece ninguna actualización a partir de junio de 2006

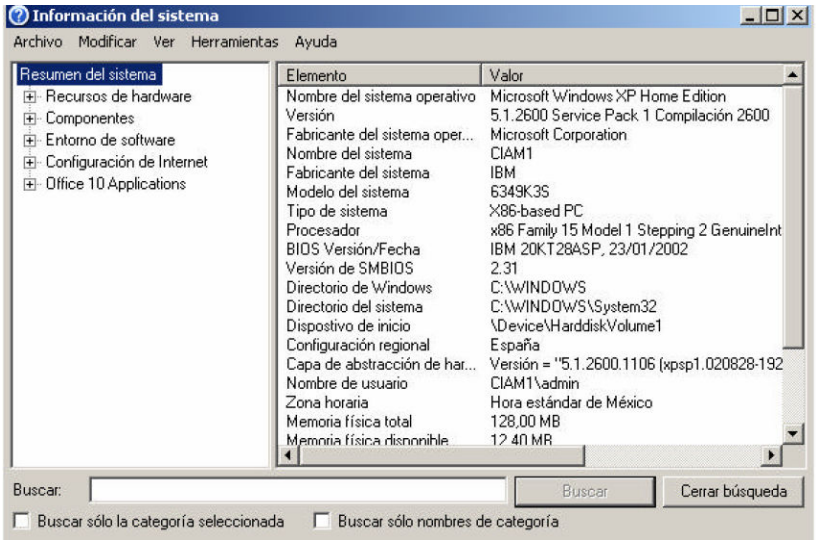
Windows 98	Sólo se ofrecen actualizaciones críticas y de seguridad a partir de agosto de 2002; no se ofrece ninguna actualización a partir de junio de 2006
Windows NT Server	No se admite a partir de diciembre de 2004
Windows NT Workstation	No se admite a partir de junio de 2004

5.9 Herramientas del Sistema

5.9.1 Información del sistema

Información del sistema recopila y muestra la información de configuración del sistema de equipos locales y remotos. Incluye información acerca de la configuración del hardware, los componentes de los equipos y el software, incluyendo los controladores firmados y los no firmados. Cuando los técnicos de soporte tengan que solucionar problemas de configuración en un sistema, necesitarán información específica acerca del equipo. Puede utilizar Información del sistema para encontrar rápidamente la información necesaria para resolver el problema. La ubicación de este comando es: **inicio/todos los programas/accesorios/herramientas del sistema**.

En la siguiente figura el árbol de categorías del panel izquierdo contiene elementos en una vista de carpetas similar al Explorador de Windows. El panel de detalles del lado derecho de la ventana muestra información acerca de los elementos que se seleccionan en el árbol de categorías.



Resumen del sistema es la primera categoría del árbol de categorías de Información del sistema. El panel de detalles muestra información general acerca de un equipo y de su sistema operativo. Puede ver información acerca del nombre, versión, fabricante y ubicación del directorio del sistema operativo. Puede comprobar la versión del BIOS o el EFI, el tipo de procesador y la información de la memoria.

La categoría **Recursos de hardware** de Información del sistema muestra información acerca de la asignación de los recursos y los posibles conflictos de uso compartido entre los recursos DMA, hardware forzado, E/S, canales IRQ y memoria.

La categoría **Componentes** de Información del sistema contiene información acerca de los siguientes componentes:

- ✓ Multimedia
- ✓ CD-ROM
- ✓ Dispositivo de sonido
- ✓ Pantalla
- ✓ Infrarrojos
- ✓ Entrada
- ✓ Módem
- ✓ Red
- ✓ Puertos
- ✓ Almacenamiento
- ✓ Impresión
- ✓ Dispositivos con problemas
- ✓ USB

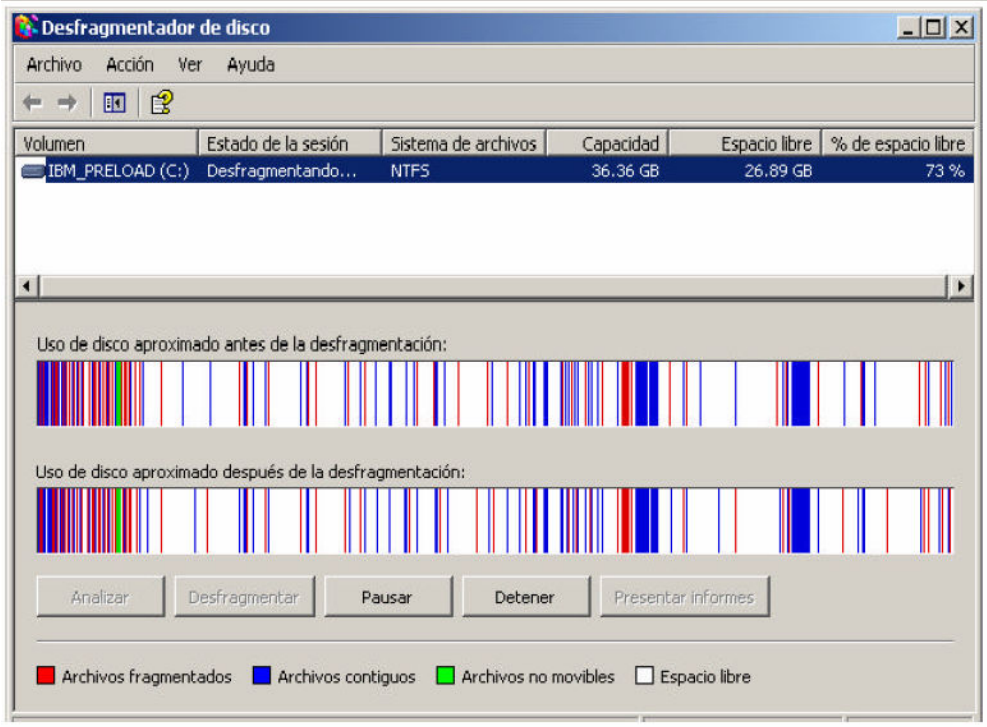
La categoría **Entorno de software** de Información del sistema contiene información acerca de la configuración, incluyendo detalles de los controladores del sistema, las variables de entorno y los trabajos de impresión actuales.

La categoría **configuración de Internet** muestra la versión y las características de nuestro navegador de Internet

5.9.2 Uso del desfragmentador

Desfragmentador de disco analiza los volúmenes locales, y consolida las carpetas y los archivos fragmentados de modo que cada uno ocupe un único espacio contiguo en el volumen. Como consecuencia, el sistema podrá tener acceso a los archivos y las carpetas y guardar los nuevos de forma más eficaz. Al consolidar los archivos y las carpetas, Desfragmentador de disco también consolida el espacio libre de un volumen, lo que hace menos probable la fragmentación de los archivos nuevos. El proceso de consolidar las carpetas y los archivos fragmentados se denomina desfragmentación. La ubicación de esta herramienta es: **inicio/todos los programas/accesorios/herramientas del sistema**

- ✓ Antes de desfragmentar archivos o carpetas, consulte Lista de comprobación: desfragmentar volúmenes.
- ✓ Para obtener sugerencias acerca de cómo utilizar Desfragmentador de disco, consulte Prácticas recomendadas.
- ✓ Para obtener ayuda acerca de tareas específicas, consulte Cómo.
- ✓ Para obtener información general, consulte Conceptos.
- ✓ Para obtener instrucciones acerca de cómo solucionar problemas, consulte Solucionar problemas.

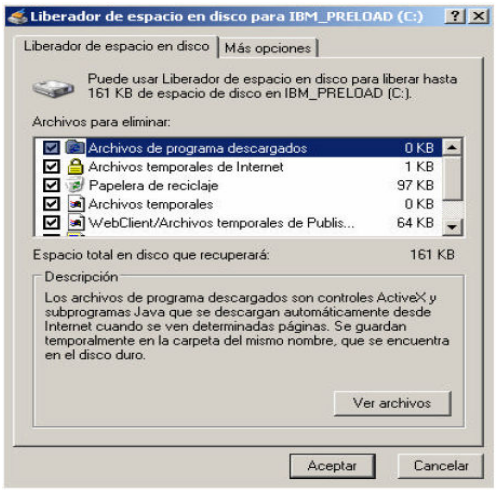


Desfragmentador

5.9.3 Liberador de Espacio en Disco

Se encarga de liberar espacio en el disco duro. La información que elimina es aquella que se acumula de archivos de programas descargados, archivos temporales de Internet, papelera de reciclaje etc. Y que no están siendo utilizados por el sistema operativo o por algún programa. Ubicación: **inicio/todos los programas/accesorios/herramientas del sistema.**

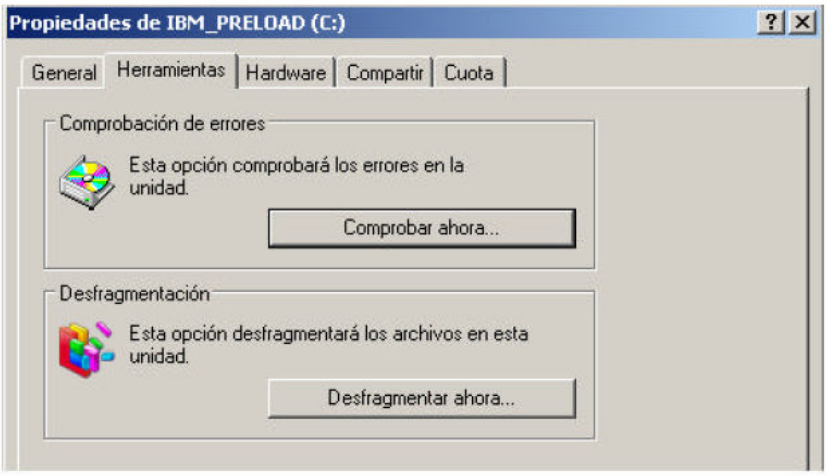
Para elegir los archivos a eliminar seleccionamos la casilla de la izquierda. Antes de eliminar lo seleccionado podemos ver una breve descripción en la parte inferior de la ventana. Para terminar con la operación debemos dar clic en aceptar. Se recomienda eliminar todos los archivos que muestra esta herramienta.



Liberador de espacio

5.9.4 Comprobación de Errores

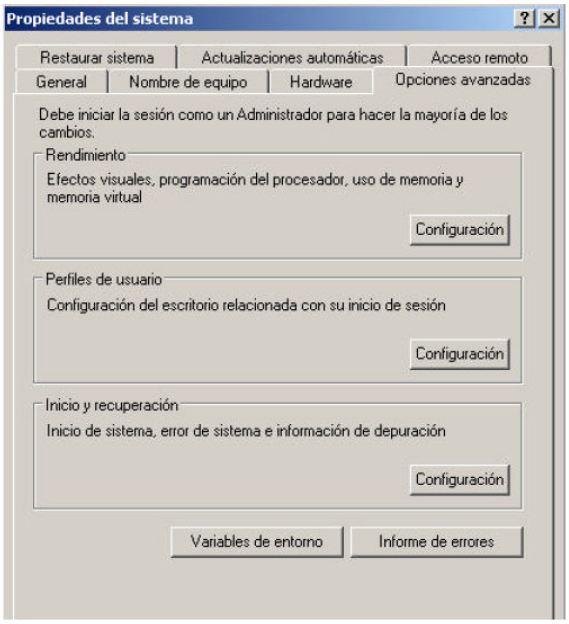
Comprobación de errores realiza una inspección física de nuestro disco duro, con el fin de detectar algún problema ya sea en el sistema de archivos o en los sectores del disco. La utilización de esta herramienta contribuye al buen funcionamiento del disco duro y por consecuencia del sistema operativo Windows. Para acceder a esta herramienta se elige la opción propiedades del disco duro.



Comprobación de errores

5.9.5 Optimizar el rendimiento

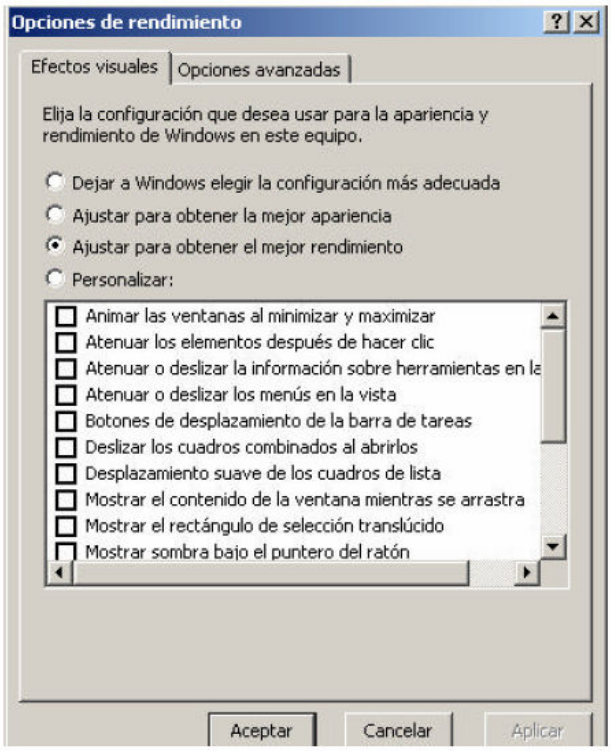
Esta opción se encuentra dentro de propiedades del sistema, en la carpeta de opciones avanzadas (clic con el botón derecho del mouse al icono de MiPC). Tiene como fin ajustar efectos visuales, optimizar la memoria, establecer perfiles de usuario, opciones de inicio y recuperación, para tener un mejor rendimiento de los programas y la memoria RAM.



Optimizar el rendimiento

Si lo que estas buscando es obtener el mejor rendimiento de la computadora, debes ir a la ficha “efectos visuales” y elegir la opción *ajustar para obtener el mejor rendimiento* y

después dar un click es aplicar, por unos segundos aparecerá una pantalla de Windows que los cambios que ordenamos se están efectuando acabo, al final notaremos como nuestra interfaz de Windows cambia de color y de efectos. Para volver a la configuración anterior hay que volver entrar a la ficha “efectos visuales” y seleccionar la opción que estaba antes.



Obtener el mejor rendimiento

5.9.6 Configurar menú de inicio.

El menú de inicio permite acceso rápido a los programas que están instalados en nuestra computadora. Para poder modificar el menú de inicio debemos darle un click con el botón derecho del mouse al botón INICIO, y elegir la opción propiedades. Hay dos formas de menú de inicio *clásico y normal*. Esta opción es muy útil, porque hay muchos programas que no ocupamos y que debemos ocultar para no saturar o para evitar que otros usuarios los utilicen y pueda desconfigurar nuestro equipo.

Nota: Esta opción es recomendable para usuarios con mayor experiencia en el manejo del sistema operativo.

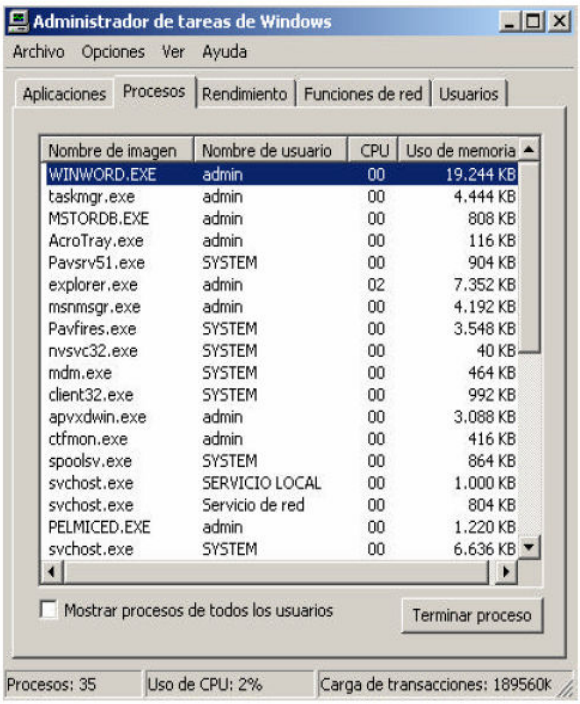
5.9.7 Administrador de tareas.

El administrador de tareas se utiliza principalmente para cerrar una aplicación que no responde, además para bloquear o cambiar la contraseña del equipo. Las opciones del administrador de tareas son:

- Aplicaciones.- Muestra todas las tareas con las cuales esta trabajando el usuario y su estado. Para terminar una tarea hay que seleccionarla y oprimir el botón finalizar tarea.
- Procesos.- Muestra todos los programas que esta utilizando la computadora, para trabajar.

- Rendimiento.- Muestra en que porcentaje esta siendo utilizado el CPU.
- Funciones de red.- Muestra la conexión y velocidad de Internet que tiene nuestro equipo.
- Usuarios.- Muestra a los usuarios que están utilizando la computadora.

Para abrir esta aplicación “administrador de tareas” hay que presionar al mismo tiempo las teclas ctrl.+alt+sup.



Administrador de Tareas

5.10 Importancia de los cortafuegos

El siguiente punto especialmente importante es contar con un buen cortafuego instalado en nuestro equipo. En el mercado, podemos encontrar decenas de ellos, algunos tremendamente especializados, como ***Tiny Firewall 2005 Professional*** (www.tiny software.com), y otros más destinados al usuario residencial. En este último grupo, resultan especialmente recomendables las *suites* de seguridad informática de empresas como **McAfee** (*Internet Security 2005),* **Panda** (*Platinium Internet Security*) o **Symantec** (*Norton Internet Security 2005*). Estas aplicaciones, además de adjuntar un cortafuegos de uso accesible y sencillo para la mayor parte de los usuarios, ofrecen otras funcionalidades como el antivirus, el filtro de correo basura e incluso filtros web para impedir el acceso a *sites* no recomendables para los más pequeños de la casa.

Aún así, existen algunas interesantes alternativas si los que buscamos es un cortafuego aunque sin invertir ni un peso. En este sentido, mencionaremos dos propuestas recomendables. La primera es **Outpost Firewall Free 1.0**, que podemos descargar de manera gratuita desde *www.agnitum.com* Esta aplicación, además de proteger nuestros puertos de red o conexión a Internet, incluye funcionalidades básicas contra los mensajes emergentes o el correo basura, aunque no son sus verdaderos puntos fuertes. La segunda

herramienta gratuita es **Sygate Personal Firewall 5.6,** que podemos descargar libremente desde *smb.sygate.com* Este cortafuegos es más complejo que el anterior, por lo que exige ciertos conocimientos de redes TCP/IP. Sin embargo es una buena alternativa cuando lo que se requiere es proteger fundamentalmente una conexión de red.

5.11 Sortear troyanos y similares

Todos los programas explicados en el punto anterior acceden a nuestro sistema, en casi la totalidad de los casos, a través del Internet o de aplicaciones aparentemente serias descargadas de la Red. Así, la primera regla de oro es que jamás autoricemos la instalación de un certificado de seguridad o la ejecución de un programa no solicitado o que provenga desde un sitio que no sea de total y absoluta confianza. De hecho, muchos de estos programas, al instalarse, crean los famosos dialers de tarificación especial, que por suerte cada vez son menos peligrosos gracias a la proliferación de las líneas ADSL que prescinden del clásico módem analógico.

Otro punto importante será no hacer clic nunca sobre ventanas de publicidad no confiables o que busquen una respuesta del usuario. Muchas veces el clásico **YES o NO** llevan al mismo punto: la descarga e instalación del código maligno. Por ello, siempre cerrar la ventana pulsando la X de la parte superior derecha de la ventana, que es un control exclusivo del sistema operativo.

Ahora bien, otra fuente de infección bastante frecuente es, aunque muchos usuarios no lo saben, software convencional que instalamos en nuestro sistema sin mayor temor o sospecha. Uno de los casos más famosos de Internet es la conocida utilidad de descargas **P2P Kazaa**, que añade durante su instalación diversas utilidades publicitarías y de ***Spyware*** sin que el usuario pueda hacer nada. Además, generalmente, aunque estos componentes se eliminen manualmente, la aplicación dejará de funcionar. Otros ejemplos similares son Real Placer o el reproductor oficial de DivX.

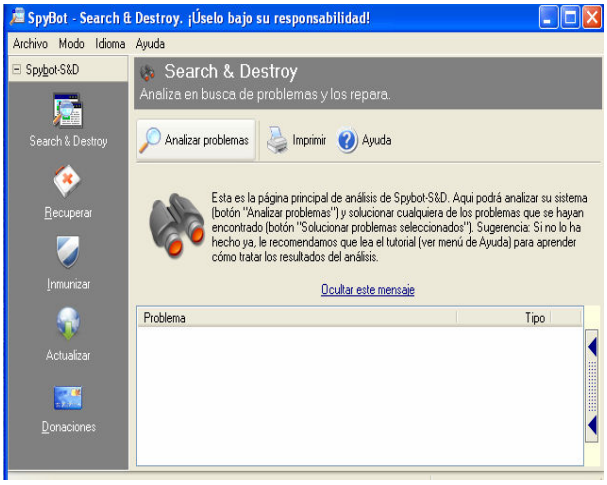
5.12 Eliminar Ad-Spy-Mal-ware

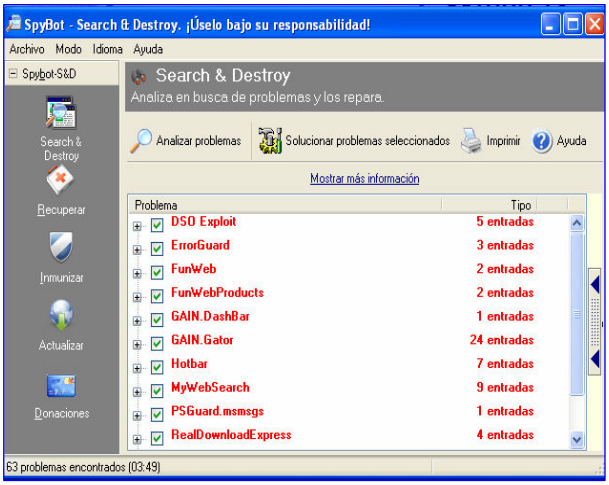
Llegados a este punto, sólo nos queda informar sobre cómo eliminar estos incómodos elementos de nuestro equipo que ralentizan la conexión a Internet, generan fallos inexplicables en el sistema, o hacen que la velocidad de arranque y proceso se reduzca drásticamente. Empezaremos por decir que, si buscas información más amplia acerca de todo este mundo, te recomendamos visitar la web ***www.spywareguide.com,*** donde, además de encontrarnos una biblioteca con miles de aplicaciones y desarrollos de *spyware* y similares, podremos realizar una verificación *on-line* de nuestro sistema.

Ahora bien, si buscamos máxima eficiencia recomendamos tres aplicaciones, dos gratuitas y una de pago. Empezaremos por las gratuitas, de los que hemos elegido **Ad-Aware SE**, todo un clásico en este campo con un elevada capacidad de detección y eliminación de código y programas malignos que puedes obtener desde ***www.lavasoft.nu*** Además, al igual que un antivirus, cuenta con un fichero de firmas que ha de actualizarse periódicamente para mantenerse al día.

El segundo software que no exige previo pago es **Spybot S&D,** que podemos conseguir desde ***www.safer-networking.org*** (web disponible en español). También similar a un antivirus, ofrece un aspecto gráfico menos cuidado, pero sorprende a la hora de detectar y eliminar algunos de los códigos más complejos. También cuenta con actualizaciones regulares.

Para terminar, entre el maremagno de herramientas disponibles en Internet para la exterminación de estas lacras, hemos seleccionado una que nos gusta especialmente por su buena terminación, excelentes resultados en la detección y eliminación y buena velocidad de funcionamiento. Se trata de **ScanSpayware** (www.scanspyware.net), y ofrece mayores funcionalidades y capacidades para hallar incluso hasta los *keyloggers* o capturadotes de las teclas que pulsamos con el teclado. La versión de prueba permite la detección, pero no la eliminación, función que sí completa la de pago (29.95 dólares).





5.13 Antivirus, nuestro aliado

Por todos es sabida la importancia de contar con un buen antivirus instalado en el sistema. Gracias a él, estaremos a salvo de cientos de amenazas que pueden llegarnos cada día en forma de mensajes de correo con adjuntos perniciosos (la primera vía de infección en estos momentos), a través de una conexión de red insegura o de una vulnerabilidad del sistema o, simplemente, por la ejecución de un fichero o programa infectado.

Nuevamente, en este sentido, volveremos a recomendar las *suites* de seguridad de empresas como **McAfee, Panda, BitDefender, Hauri(ViRobot), Trend Micro Pc-cillin, Kaspersky Antivirus, F-secure antivirus, Avast antivirus o Symantec(Norton Antivirus)**, que con precios aceptables aseguran nuestra máquina y posibilitan actualizaciones prácticamente a diario contra nuevos desarrollos malignos que surjan. En este aspecto, vale la pena recordar las nuevas tecnologías **TruPrevent** introducidas por Panda con sus últimos productos. Gracias a ellas, además de comportarse como un antivirus/cortafuegos convencional, el programa analiza el sistema en busca de sucesos fuera de lo normal, tales como la ejecución de procesos sospechosos, utilización de áreas de memoria reservada, etc. De esta manera, los programas de esta compañía que emplean dicha tecnología son capaces de enfrentarse a amenazas desconocidas con enorme precisión, evitándonos problemas posteriores.

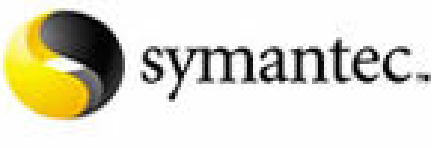
Ahora bien, como ocurre en casi todos los ámbitos, también en éste existe alternativas gratuitas, también en éste existen alternativas gratuitas. Aquí, quizá uno de los antivirus de uso libre más conocido es **Antivir Personal Edition,** que podemos descargar desde ***www.free-av.com*** en versión para Windows. Linux, Open BSD, FreeBSD o Solares, incluye algunas de las funciones más habituales de los productos de pago, aunque su ritmo de actualización sea menor que el de muchas propuestas comerciales. Sin embargo, no podemos olvidar que no cuesta absolutamente nada y, por tanto, no cuesta absolutamente nada y, por tanto, no se puede pedir mucho más. Tampoco olvides que, además de la alternativa gratuita, en la web de Panda Software (www.pandasoftware.com) podemos ejecutar sin inversión alguna y *on-line* el software Panda ActiveScan.

Antes de elegir debemos tener en cuenta si lo queremos para una computadora o para ser instalado en un servidor, que se pueda instalar en el sistema operativo que estamos utilizando, que se pueda actualizar de manera fácil y rápida, que cuente con una página Web de soporte y que sea original. Los Antivirus antes mencionados no consumen muchos recursos del sistema operativo (excepto el Norton y McAfee) y son muy efectivos en la detección de nuevos virus de diferentes tipos como: troyanos, gusanos, etc. Y cuentan con su propio Firewall.

Hay algunas páginas de antivirus que ofrecen servicio de información y escaneo de virus:

1). http://www.trendmicro.com/la/home/enterprise.htm
2). http://www.bitdefender.com/scan/license.php
3). http://www.symantec.com/region/mx/product/
4). http://alerta-antivius.red.es

Nota: todos los Antivirus deben estar actualizados día a día.

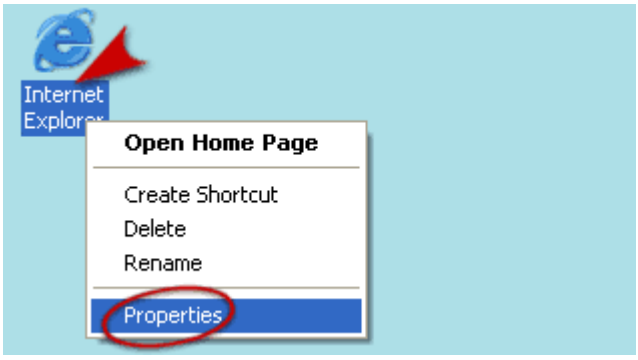


5.14 Borrando Archivos Temporales de Internet

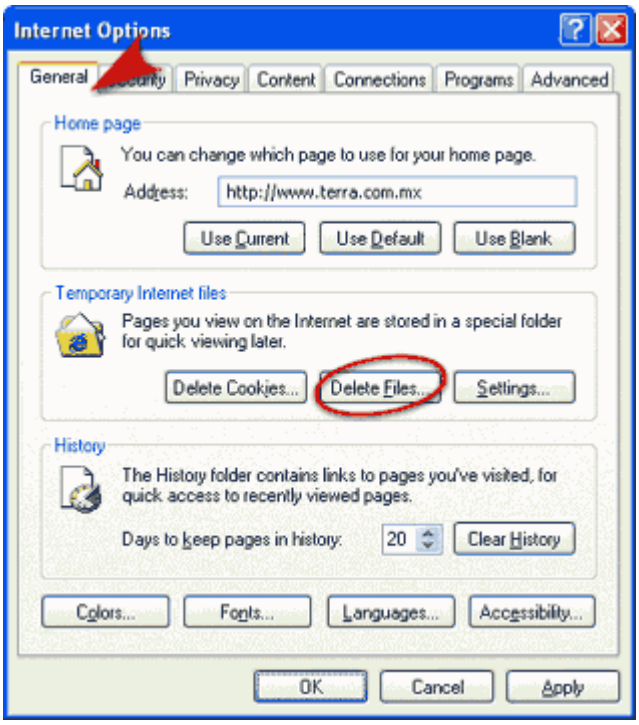
Haz espacio en tu computadora para navegar más rápido y borra los archivos temporales que pertenecen a los sitios que has visitado. Para hacer más espacio en tu computadora y navegar más rápido en Internet te recomendamos eliminar constantemente los archivos temporales de los sitios que has visitado.

A continuación te explicamos los pasos a seguir para borrar los archivos temporales de Internet:

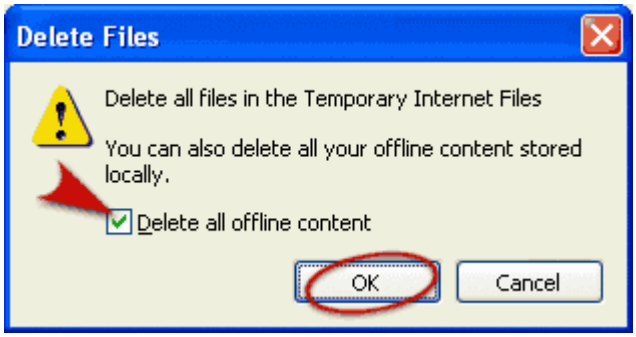
1. Ubica el cursor sobre el icono del Internet Explorer, haz click con el **BOTÓN DERECHO del mouse** y selecciona la opción de **Properties**.



2. Dentro de la pestaña **General** presionas el botón de **Delete Files...** como lo indica la imagen.



3. Aparecerá una ventana en la cual tenemos que activar la opción de **Delete all offline content** y después presionar el botón de **OK**.



Ahora si ya hiciste espacio en tu computadora y borraste muchos archivos de tu computadora que tu ni sabías que existían y no necesitabas.

5.15 Cómo borrar archivos temporales de Windows

Cierre todas las ventanas y todos los programas abiertos.

1. Desde Inicio, Ejecutar, escriba **%TEMP%** y pulse Enter.
   Nota: debe escribir también los signos "%" antes y después de "temp".
2. Cuando se abra la ventana del Explorador de Windows, pulse CTRL+E (o seleccione desde el menú "Edición", la opción "Seleccionar todo").
3. Pulse la tecla SUPR y confirme el borrado de todo, incluyendo los ejecutables.
4. Pinche con el botón derecho sobre el icono de la "Papelera de reciclaje" en el escritorio, y seleccione "Vaciar la papelera de reciclaje".

NOTA: Si se recibe un mensaje de que no se puede borrar todo, reinicie Windows en modo a prueba de fallos, como se indica en el siguiente artículo, y repita todos los pasos anteriores:

5.16 Cómo proteger los datos para prevenir su pérdida.

Todos poseemos datos importantes en nuestros ordenadores que quisiéramos no perder, desde documentos de trabajo a fotos personales pasando por datos de programas. Sin embargo no podemos creer que se encuentren "a salvo" dentro de ellos.

Todo lo almacenado en un disco duro esta expuesto a múltiples peligros. Virus, fallos físicos del equipo, errores del sistema e incluso problemas ocasionados por los propios usuarios son un peligro potencial. Cualquiera de estos casos y otros tantos más pueden ocasionar la pérdida o daño irreparable de los datos. Para evitarlos, o al menos para tener la seguridad de que serán hasta cierto punto remediables, hay que tomar unas medidas básicas de seguridad.

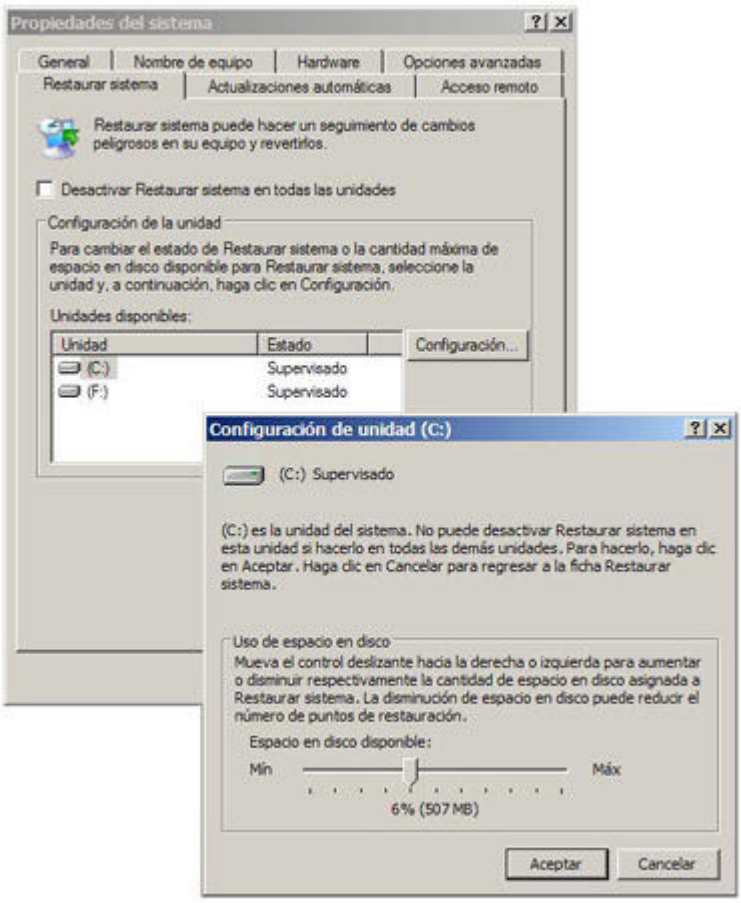
5.16.1 Puntos de Restauración de Sistema en Windows

En los sistemas Windows existe una opción de gran utilidad para la salvaguarda de los datos propios de Windows y de los programas instalados, la llamada Restauración de Sistema. Ésta permite deshacer los cambios realizados y volver al estado anterior sin mayor pega.

Para que esto sea posible se han de crear puntos de restauración, es decir fechas en las que se guarda el estado del sistema para poder ser utilizadas posteriormente. Estos puntos han de ser creados cada periodos de tiempo prudencial y antes de realizar cambios drásticos en el sistema que conlleven algún peligro.

Para activar la restauración de sistema accederemos al Panel de control y al icono de Sistema que nos mostrará una ventana nueva con diferentes pestañas. Dentro de la pestaña "Restaurar Sistema" veremos un cuadro llamado Desactivar Restaurar sistema en todas las unidades, este ha de estar desmarcado para poder utilizar los puntos de restauración.

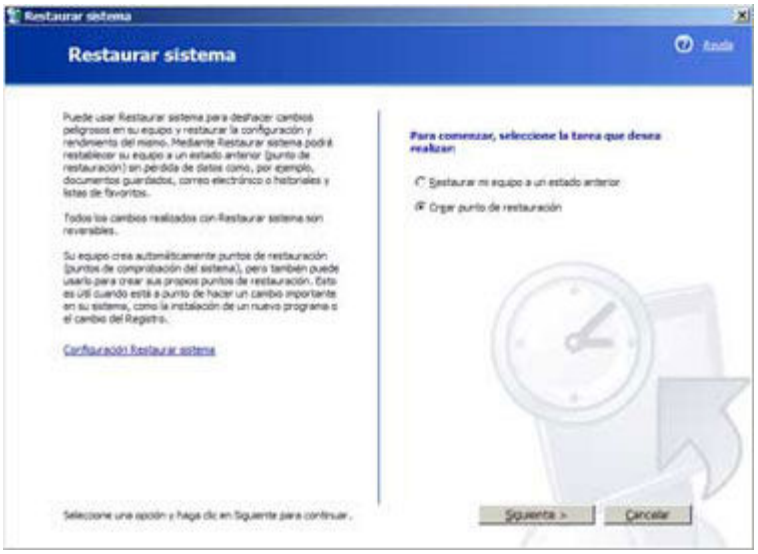
Normalmente esta opción viene desactivada por defecto. Una vez hecho esto Windows creará él mismo los puntos.



En esa misma pestaña aparecerá una lista de las unidades de disco de nuestro ordenador. Marcando cada una de ellas y con el botón de propiedades accederemos a la posibilidad de escoger el tamaño de disco que permitimos a Windows que use para hacer los puntos de restauración. Cuanto mayor espacio de disco le asignemos más habitualmente creará puntos de restauración. Se debe escoger un punto intermedio, lo suficientemente seguro para que las actualizaciones se hagan periódicamente pero no excesivo y que nos reste una gran capacidad.

A parte de los puntos de restauración periódicos, como comentábamos antes, es muy importante crear puntos cuando se realicen cambios críticos en el sistema (instalaciones de aplicaciones, de controladores, de hardware nuevo).

Para crear un punto de restauración el mecanismo es sencillo. Se accederá a Todos los programas -> Accesorios -> Herramientas de Sistema -> Restaurar sistema. Esto nos mostrará un cuadro de dialogo con toda la información necesaria. Seleccionaremos la tarea de Crear un nuevo punto de restauración y hacemos clic en Siguiente. En el siguiente paso escogeremos un nombre para el punto de restauración. Es muy útil que el nombre sea descriptivo para saber a que momento pertenece cada uno a la hora de hacer una restauración. Podemos llamarle "Antes de instalar X programa". Para finalizar el proceso aceptaremos haciendo clic en Crear. Así tendremos nuestro punto de restauración creado.



Restaurador de sistema

Si lo que deseamos es volver a un punto de restauración ya creado los pasos son parecidos. Accederemos a Todos los programas -> Accesorios -> Herramientas de Sistema -> Restaurar sistema y en esta ocasión marcaremos Restaurar mi equipo a un estado anterior. En la siguiente pantalla elegiremos la fecha del punto de restauración deseado y aceptaremos.

Si los problemas del sistema fueran lo suficientemente graves para que Windows no pudiera arrancar correctamente el modo de acceso a un punto de restauración es también sencillo. Pulsaremos la tecla F8 durante el arranque del equipo y esto desplegará un menú. En él escogeremos "última configuración válida conocida" y Windows arrancará con el estado del punto de restauración más cercano en el tiempo que funcione correctamente.

5.16.2 Imágenes del disco duro y Norton Ghost

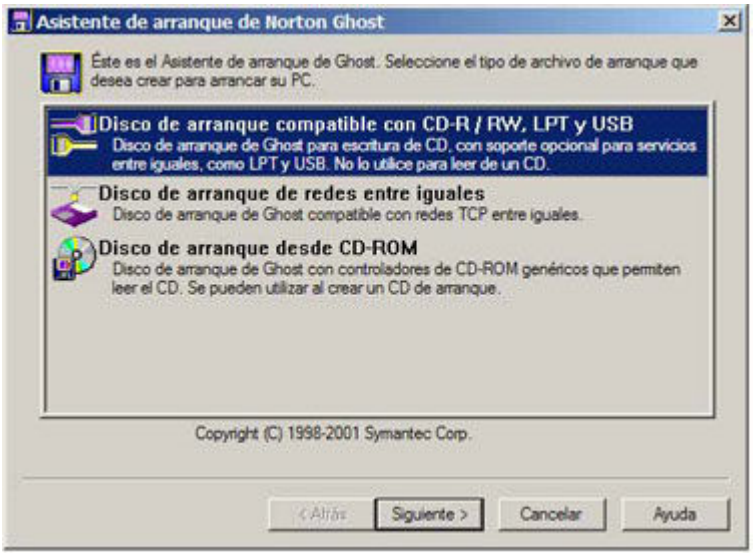
Una imagen de un disco, ya sea un CD, diskette, disco duro, etc., es una copia exacta del original guardada en otro medio. Su uso habitual es la salvaguarda de datos en el estado exacto del original o la copia idéntica de ellos.

Existen múltiples utilidades creadas para obtener imágenes de los discos duros. La más extendida es el Norton Ghost (http://www.symantec.com/sabu/ghost/ghost_personal/) y será la que comentemos en este tutorial.

Una opción especialmente recomendable a la hora de preservar la integridad del Sistema Operativo y los programas instalados en nuestro ordenador es crear una imagen de ellos. Así si surgiera algún problema o deseásemos formatear el disco duro tardaríamos breves instantes en devolver la copia a su lugar y solucionar todos los problemas.

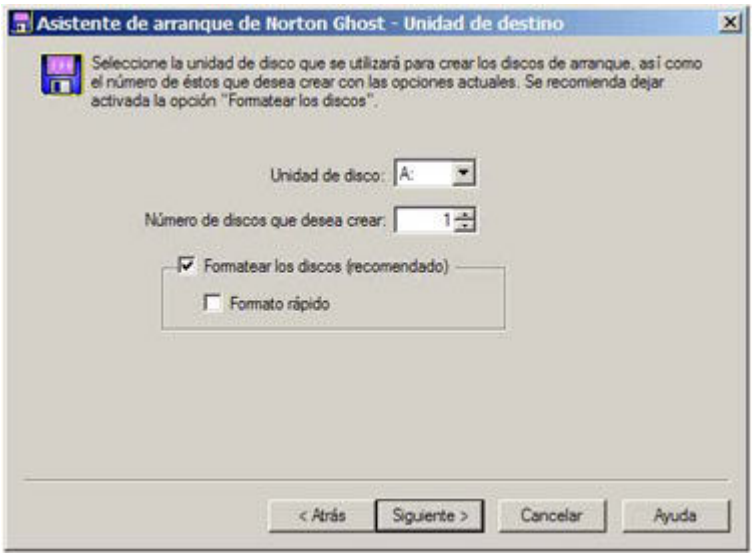
Norton Ghost nos ayuda en esta tarea y tiene un uso muy sencillo a demás de contar con tutoriales integrados que nos guiaran paso a paso. Éste programa es compatible con sistemas de archivos FAT, NTFS y EXT2 y no requiere grandes prestaciones técnicas del equipo. Sus requisitos mínimos son un 386 con 8Mb de RAM y un sistema Windows 98/NT 4.0 o superior.

Para hacer funcionar el Norton Ghost comenzaremos instalándolo en nuestro ordenador y ejecutando el "Asistente de arranque de Norton Ghost" para obtener un diskette que nos permita usar el programa. Esto nos abrirá una nueva ventana en la que marcaremos "Disco de arranque compatible con CD-R/RW, LPT y USB" y pulsaremos siguiente. En el nuevo paso escogeremos las opciones referidas a nuestro sistema, lo más habitual será dejar todas desmarcadas a no ser que se cuente con unidades SCSI.



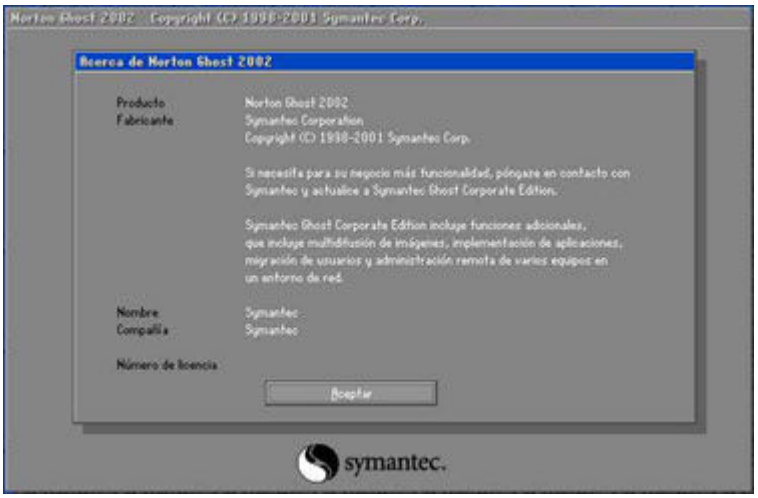
El diskette de Norton Ghost puede funcionar con un sistema PC-DOS o MS-DOS a la hora de arrancar. El sistema PC-DOS viene ya incluido con el programa y servirá perfectamente, si se quisiera utilizar MS-DOS pulse el botón de "Obtener MS-DOS" con un diskette formateado insertado en la unidad.

El paso siguiente nos muestra la ruta en la que se encuentra el archivo GhostPE.exe que será el encargado de crear los diskettes. Normalmente la ruta predefinida será la correcta, si no es así pulse Examinar y seleccione la ubicación del archivo. Pulsando siguiente llegamos a las opciones de grabación del diskette. Marcaremos la unidad (habitualmente A:), el número de copias y permitiremos que el programa formatee el disco por seguridad.



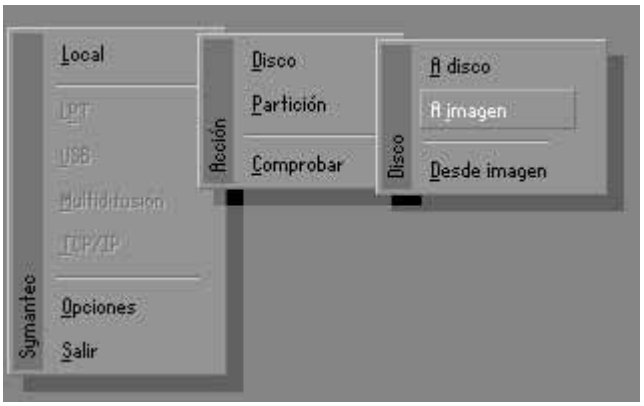
Una vez hecho esto se nos mostrará una pantalla de revisión de las opciones que hemos escogido para ver si son correctas y proceder a la grabación. El siguiente paso es el formateo del diskette que aceptaremos y una vez acabado cerraremos. Acto seguido Norton Ghost comenzará a crear el diskette y en unos instantes estará terminado.

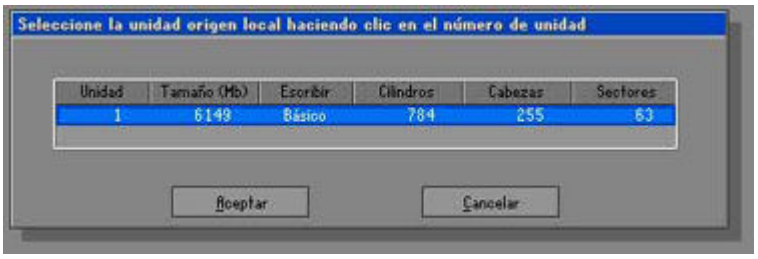
La razón del uso del diskette de arranque es sencilla, no podríamos crear una imagen exacta del sistema si estuviera en funcionamiento. Así que el siguiente paso será arrancar el ordenador con este disco. Reinicie el ordenador con el disco insertado y espere a que arranque. Si esto o ocurriera y se iniciara Windows significará que el orden de booteo es incorrecto. Para solucionarlo habrá que acceder a la configuración de la BIOS (habitualmente con la tecla suprimir en el arranque) y allí colocar la diskettera como primera unidad de booteo.



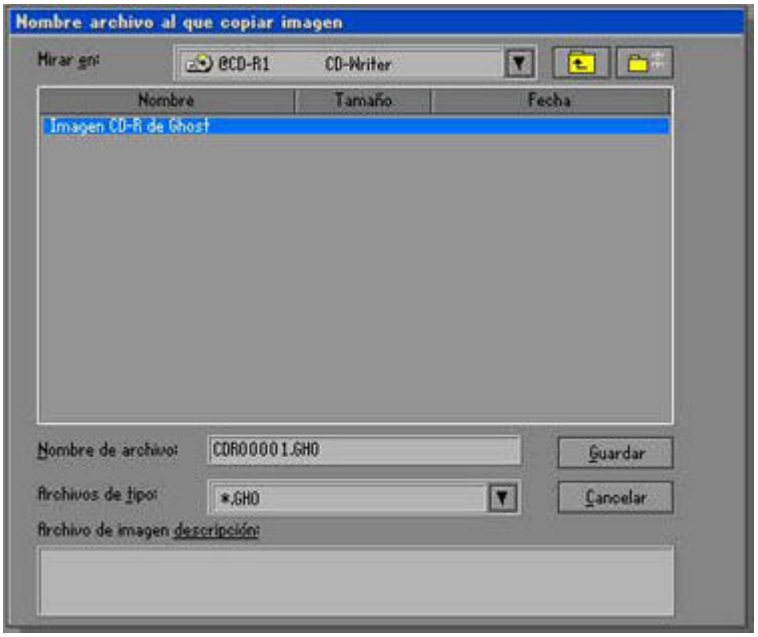
Cuando el ordenador rearranque correctamente nos llevará a una pantalla introductoria de Norton Ghost. De ella será de utilidad mantener a mano el número de licencia para más adelante. Nos encontraremos al aceptar en un entorno grafico con un menú. Para iniciar la clonación del disco escogeremos Local -> Disco -> A imagen. Seleccionaremos en el menú la unidad concreta de la que queremos hacer la imagen (si es

que hubiera varias) y aceptaremos. El siguiente paso será escoger la unidad en la que se grabará la imagen. Recomendamos un CD o DVD grabable para guardar la imagen.





El nombre del archivo creado *.GHO no puede ser modificado por el usuario pero si la descripción inferior. Servirá de ayuda para especificar de que hemos creado la imagen: "disco C: en Agosto" o "sistema recién instalado en el 2003" son maneras útiles de usar la descripción para conocer el contenido de la imagen. Una vez hecho pulsaremos el botón Guardar.

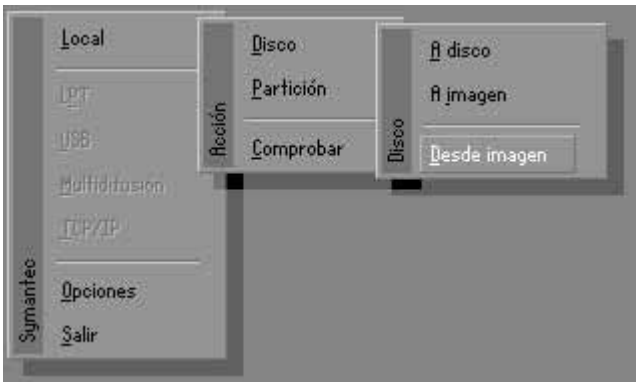


El archivo de imagen creado puede guardarse en un formato comprimido. Según nuestras necesidades así escogeremos si queremos dejarlo descomprimido, hacer una compresión mínima, o reducir el archivo al máximo posible. Junto con esto se nos ofrecerá la útil opción de guardar junto a la imagen una copia del diskette de arranque, la cual aceptaremos.

En este momento Norton Ghost comenzará a crear la imagen. Es muy probable que la imagen que se intente guardar sea superior al tamaño del soporte que se posee. Por ejemplo guardar los datos de una partición de 1Gb en CDs de 650Mb. El programa dividirá automáticamente el archivo de imagen en partes del tamaño del disco y cuando haya acabado pedirá el siguiente disco. El proceso de volcado tomará bastante tiempo. Una vez finalizado podremos salir del asistente haciendo clic en Salir dentro del menú principal.

Por supuesto, si se deseara guardar la imagen en otro disco duro o partición el proceso será el mismo pero escogiendo en vez de la unidad de CD la de disco.

El proceso contrario es restaurar una imagen al disco duro, el proceso es similar. En el menú escogeremos Local -> Disco/Partición -> Desde imagen. Esto nos llevara a un cuadro de dialogo en el que escogeremos la ubicación del archivo de imagen. El paso siguiente será escribir el número de licencia del programa para poder continuar. Una vez hecho esto habremos de elegir la unidad de destino en la que introduciremos los datos de la imagen. En el cuadro de Detalles de la unidad de destino confirmaremos la disposición de las particiones del disco duro y aceptaremos.



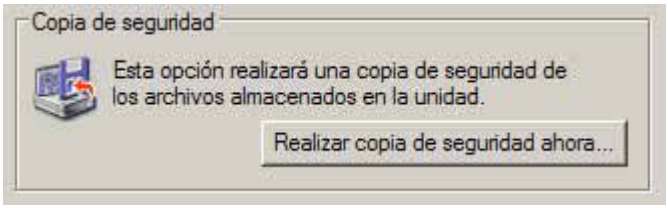
A partir de entonces Norton Ghost restaurará la imagen al disco duro sobrescribiendo todo lo que pudiera haber en él. Si la imagen ocupara más de un disco los irá pidiendo por si mismo en orden. Una vez terminada la operación el último paso será reiniciar el ordenador para que el sistema cargue desde la unidad restaurada.

Se recomienda pasar alguna utilidad para comprobar la integridad de la imagen restaurada. Scandisk o similares servirán.

5.16.3 Utilidad de copia de seguridad de Windows

El propio Windows nos ofrece una aplicación con la que realizar copias de seguridad. Para acceder a ella sólo hace falta entrar en las propiedades del disco duro con el botón

derecho sobre él dentro del explorador de archivos (dentro de Mi Pc). Una vez allí en la pestaña de Herramientas tendremos la opción de realizarlas.



El modo asistente nos ayudará en todo el proceso. En la primera pantalla escogeremos Efectuar una copia de seguridad de archivos y configuración y avanzaremos con el botón Siguiente. Entonces deberemos escoger qué archivos guardaremos en nuestra copia de seguridad. Se nos plantean cuatro opciones, los documentos y preferencias del usuario actual, los de todos los usuarios, toda la información del disco duro, o elección personalizada. Si ninguna de las predefinidas nos satisface continuaremos escogeremos ésta última que nos desplegará un cuadro de diálogo donde escoger personalmente los archivos.

En la pantalla siguiente escogeremos una ubicación donde guardar el backup (un archivo *.bkf). Como predefinido tenemos la unidad A: pero con el botón Examinar podremos especificar la ubicación que deseemos. Él último cuadro de diálogo nos mostrará las opciones que hemos elegido por si hubiera algún error. Con Finalizar comenzará el proceso de copia de seguridad que según la cantidad de datos llevará un tiempo determinado.

El proceso inverso (recuperación de una copia de seguridad) es prácticamente el mismo. En la primera pantalla escogeremos Restaurar archivos y configuraciones, después marcaremos la ubicación del archivo de backup y dejaremos que Windows finalice el proceso de reposición de los archivos.

También es posible acceder a esta utilidad desde Inicio >> Programas >> Accesorios >> Herramientas del sistema.

5.16.4 Backups y copias de seguridad

Conociendo ya el modo de mantener a salvo el sistema y los programas solo nos queda hablar de los archivos guardados en nuestro equipo. Hacer una copia de respaldo de ellos cada cierto tiempo será la única manera de mantenerlos a salvo.

Los soportes más habituales para las copias de seguridad son los ópticos como CDs y DVDs y los magnéticos como cintas, unidades ZIP, etc. así como los discos magneto-ópticos (MO). A nivel personal los más extendidos los CD-R y CD-RW, discos compactos grabables y regrabables. La copia y almacenamiento de los datos de forma periódica en unidades de este tipo evita los riesgos de pérdidas.

CONCLUSIONES

Para finalizar podemos concluir lo siguiente.

- La Dirección General de Televisión Educativa tiene la tarea de producir, programar y transmitir contenidos a través de la Red EDUSAT, pero para llevar a cabo esto se apoya en una de las herramientas que actualmente se han hecho indispensable en la vida cotidiana de todos nosotros, desde la casa hasta la oficina, me refiero a la computadora; hay aproximadamente 400 equipos informáticos los cuales deben estar en buenas condiciones y en perfecto funcionamiento para lograr que la DGTVE cumpla con su misión y objetivos establecidos.

- Para esto, la institución cuenta internamente con una Coordinación de Informática y en específico un área de Soporte Técnico que se encarga de la evaluación y determinación de requerimientos de equipo de cómputo, el diseño y desarrollo de una red de información interna, asesoría a usuarios para el manejo de sistemas, así como la conservación y revisión (mantenimiento preventivo y correctivo) periódico de los aparatos a su cargo.

- Así como a un Automóvil para que puede realizar su función que es la de transportarnos de un lugar a otro, se deben de tener cuidados especiales(revisar si tiene aceite, gasolina, liquido para frenos, que este limpio por dentro y fuera, que funcionen las luces, etc.) y realizarlos con una periodicidad constante, pues bien un Ordenador Personal (PC) se le debe de estar revisando constantemente para optimizar su uso, entre los procesos que se le deben de hacer podemos mencionar el actualizar el sistema, eliminar los archivos temporales que el mismo equipo genera ya que ocupan espacio en el disco duro y consumen recurso de Memoria RAM, la limpieza interna y externa de la máquina (liberación del polvo) y el constante scaneo en busca de amenazas informáticas (virus, gusanos, troyanos, spywares, spam, etc.) para esto la DGTVE cuenta con una herramienta Antivirus “El ViRobot” de la empresa Hauri y el Spybot “Search & Destroy”, ambos han resultado muy eficiente para la búsqueda y erradicación de estos y mantener a salvo todas las computadoras de la Institución.

- No importando de que fabricante se trate (IBM, DELL, COMPAQ o GENERICO) todas tienen una Arquitectura similar entre sí, y es prioritario que para darles un buen mantenimiento se deba conocer internamente y saber usar, de lo contrario, podríamos provocarle más daño que bien.

- Es imposible profundizar cada uno de estos temas en un trabajo de tesis, ya que dicha información es muy extensa haciendola aburrida y tediosa imposibilitando su compresión; esto es lo que no se quiso hacer, además ésta información no se puede ir actualizando debido al constante crecimiento y evolución de la tecnología informática y de comunicación, por ello se maneja al final una lista de fuentes consultadas para mantenerse al día o incluso ahondar lo más posible en un tema que no haya quedado claro.

REFERENCIAS DE INFORMACIÓN CONSULTADAS

- http://www.entrebits.com/trucos/mostrar/elimina-t
- http://www.vsantivirus.com/faq-mostrar-extensiones.htm
- http://alerta-antivirus.red.es
- http://dgtve.sep.gob.mx
- Gran Libro Hardware. Dembowski
- Ampliar y Reparar su PC. Schuller
- Mi PC Actualización, Configuración, Mantenimiento y Reparación. José María Martín.
- Fundamentos de Informática. Luis A. Ureña – Antonio M. Sánchez – María T. Martín – José M. Matas.
- PCactual. Fernando Claver. Número 175.
- La Electrónica de las Computadoras. Ing. Horacio D. Vallejo. Editorial Quark
- Mantenimiento Preventivo y Correctivo Para PCs. Alfonso Gutiérrez Molina – Justino Peñafiel Salinas – Iván G. Villarreal Azúa. Dirección General de Servicios de Cómputo Académico (DGSCA)
- Mantenimiento Preventivo de la Computadora. M.C. Juan Manuel Clavillo Ramos. Universidad de Colima, Centro Interactivo de Aprendizaje Multimedia Campus Coquimatlán.