



LICENCIATURA EN ADMINISTRACIÓN

APUNTES

PARA LA ASIGNATURA

INFORMÁTICA BÁSICA II



2005



Colaboradores

Coordinación general

L. A.C. y Mtra. Gabriela Montero Montiel

Coordinación académica

L.A.C. Ramón Arcos González

Elaboración de contenido

David Espartaco Kanagusico Hernández
Gilberto Manzano Peñaloza
María Catalina Cariño Vázquez
Marlene Ramírez Chavero
Pedro Gutiérrez Delgado
Ramón Arcos González
Ricardo Alberto Báez Caballero

Coordinación operativa

L.A.C. Francisco Hernández Mendoza

Asesoría pedagógica

Sandra Rocha

Corrección de estilo

José Alfredo Escobar Mellado

Edición

Captura



Prólogo

labor editorial más de la Facultad de Contaduría y Administración, los materiales educativos que conforman el Paquete de Estudio Autodirigido del Sistema Universidad Abierta representan un esfuerzo encauzado a apoyar el aprendizaje de los estudiantes de este sistema.

Esperamos que estos materiales sirvan de punto de referencia tanto a los asesores como a los alumnos. A los primeros para que tengan medios que les permitan orientar de mejor manera y con mayor sencillez a sus estudiantes. Y a los segundos para que cuenten con elementos para organizar su programa de trabajo, se les facilite comprender los objetivos de cada asignatura y se sirvan de los apoyos educativos que contienen, como los esbozos de las materias y sus unidades, cuestionarios de autoevaluación, lecturas básicas de estudio, actividades de aprendizaje y apuntes elaborados por los asesores.

Así, ponemos estos materiales a disposición de nuestra comunidad, esperando que alcancen sus propósitos.

ATENTAMENTE

Ciudad Universitaria, D. F., Enero de 2006

C.P.C. y MAESTRO ARTURO DÍAZ ALONSO
DIRECTOR



Prohibida la reproducción total o parcial de esta obra, por cualquier medio, sin autorización escrita del editor.

GUIA DE ESTUDIO PARA LA ASIGNATURA INFORMÁTICA BÁSICA I

Primera edición, enero de 2006

Derechos reservados conforme a la ley.

Prohibida la reproducción parcial o total de la presente obra por cualquier medio, sin permiso escrito del editor.

DR © 2001 Universidad Nacional Autónoma de México

Facultad de Contaduría y Administración

Fondo Editorial FCA

Circuito Exterior de Ciudad Universitaria,

Deleg. Coyoacán, 04510-México, D.F.

Impreso y hecho en México



Contenido

Introducción.....	7
Objetivos generales de la asignatura	9
Unidad 1. Bases de datos, manejo y aplicación	11
Objetivos particulares de la unidad.....	12
Unidad 2. Concepto de Telecomunicaciones, virus informáticos	33
Objetivos particulares de la unidad.....	34
Unidad 3. Topología de redes	105
Objetivos particulares de la unidad.....	106
Unidad 4. Graficadores, manejo y aplicación	115
Objetivos particulares de la unidad.....	116
Unidad 5. Herramientas de presentación, manejo y aplicación.....	123
Objetivos particulares de la unidad.....	124





Introducción

La formación universitaria está íntimamente ligada al mercado laboral y cultural, es decir forma expertos y desarrolla conocimientos avanzados. Entre estos conocimientos avanzados se encuentran las nuevas tecnologías de la información y de la comunicación, requeridas casi en cualquier momento por el mercado laboral.

La capacidad para utilizar estas nuevas tecnologías permite a los alumnos tener acceso a una mayor cantidad de información y así a mayores conocimientos, y forjarse una preparación más sólida y más competitiva para su futuro profesional.

Seguramente ya estás familiarizado con los temas de la asignatura, pues a lo largo del estudio del paquete, como son las lecturas recomendadas, la guía de estudio y el cuaderno de actividades, has ido repasando los conceptos sobre bases de datos, redes, Internet y virus, PowerPoint y presentaciones electrónicas, contribuyendo así, a que tengas un mayor aprendizaje sobre los temas que contempla el programa de la asignatura. Pues bien, finalmente hemos llegado al último material del paquete: los apuntes, que como su nombre lo indica, son un resumen de los puntos esenciales de la unidades de la asignatura, y tienen como finalidad convertirse en un apoyo para



reforzar tu aprendizaje, después de haber revisado las lecturas que se te recomendaron en la guía de estudio y que constituyen la fuente primaria de estudio, pues a través de ellas, es donde profundizarás más. Por lo tanto, nuestra recomendación es que hagas uso de los apuntes después de revisar a los autores.

Los apuntes serán entonces tu último repaso antes de pedirle a tu asesor la aplicación de la evaluación correspondiente.

El material que te presentamos, buscan de una manera resumida, introducirte en el estudio y la utilización de las bases de datos, redes de computadoras, Internet, virus, Powerpoint y los graficadotes, software necesario para apoyar el campo no sólo de la Administración, sino prácticamente de todas las disciplinas, de modo que puedas conocer, explorar y explotar todas las herramientas básicas para tu trabajo tanto escolar como laboral. Esta constituido bajo una estructura ordenada donde se contemplan los objetivos tanto generales como específicos por unidad, y el desarrollo de los contenidos esta basado en cada punto del programa oficial de la asignatura.

El lenguaje que se presenta es muy sencillo y si en algún punto se usa algún tecnicismo, es que damos por hecho de que ya cuentas con conocimientos al respecto, a través de las fuentes primarias de información. Se presentan ilustraciones y las pantallas son directas de los programas, a fin de que puedas ir siguiéndolas en tu computadora e ir practicando la forma en que deben ingresarse los datos, y la forma en que deben darse las instrucciones a través de los comandos.

Esperamos que el material que aquí te presentamos, despierte tu interés, te sea de gran utilidad y se convierta en un apoyo para que puedas desenvolverte en el ambiente laboral del Licenciado en Administración.



Objetivos generales de la asignatura

Al finalizar el curso el alumno podrá hacer uso de las aplicaciones de software más comunes de propósito general (Manejadores de Bases de datos, Graficadores y Herramientas de presentación) y conocerá los fundamentos básicos de las telecomunicaciones.





Unidad 1.

Bases de datos, manejo y aplicación

1.1 Conceptos básicos.

- 1.1.1 Qué es una base de datos relacional.
- 1.1.2 Qué es un campo, un registro y una tabla.
- 1.1.3 Qué es un query.
- 1.1.4 Cómo cargar una base de datos.
- 1.1.5 Creación de una tabla.
- 1.1.6 Elaboración e impresión de reportes.

1.2 Consulta a la base de datos.

- 1.2.1 Despliegue de registros.
- 1.2.2 Selección de registros dada una condición.
- 1.2.3 Visualizar y modificar los datos de los registros de una base de datos.
- 1.2.4 Añadir registros a la base de datos.
- 1.2.5 Borrar registros de la base de datos.
- 1.2.6 Modificar la estructura de la base de datos.
- 1.2.7 Añadir datos a campos nuevos.

1.3 Elaboración e impresión de reportes.





Objetivos particulares de la unidad

Al finalizar la unidad, el alumno podrá hacer uso de las aplicaciones de **Access** software Microsoft Office. Explicara los conceptos básicos en que se fundamenta la administración de las bases de datos en un sistema de información como resultado del aprendizaje valorará sistema de procesamiento de datos; Identificará los campos de actuación profesional y los sectores en los que se busca sensibilizar al alumno sobre las ventajas proporcionadas por el manejo digital de la información.

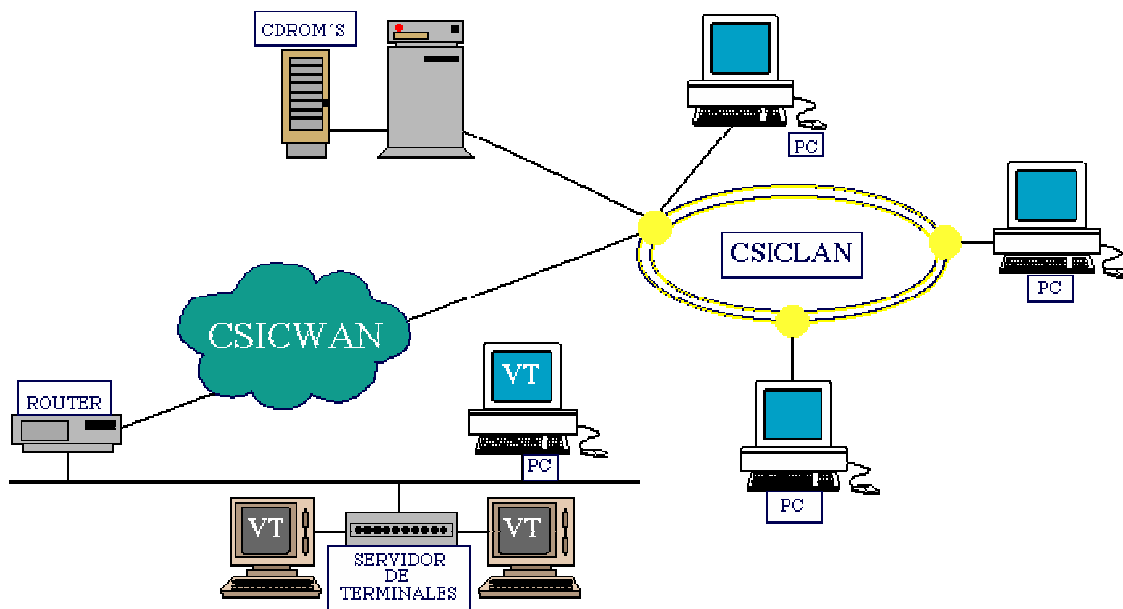




1.1 Conceptos Básicos.

La palabra datos (del latín data, plural de datum) significa simplemente “hechos” entidades independientes sin evaluar los datos pueden ser numéricos o no numéricos (por ejemplo, alfabéticos o simbólicos). La información es un conjunto ordenado de datos los cuales pueden recuperarse de acuerdo con la necesidad del usuario.

Una base de datos es una colección de archivos interrelacionados creados por un DBMS. El contenido de una base de datos se obtiene combinando datos de todas las diferentes fuentes en una organización, de tal manera que los datos estén disponibles para todos los usuarios, y los datos redundantes puedan eliminarse, o al menos minimizarse.

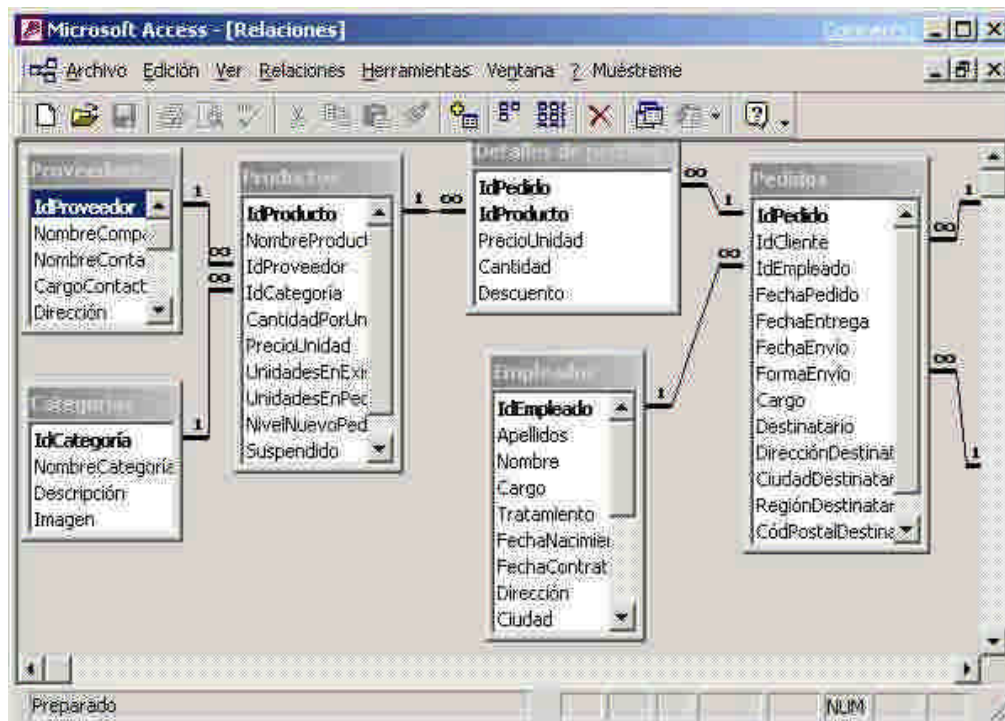
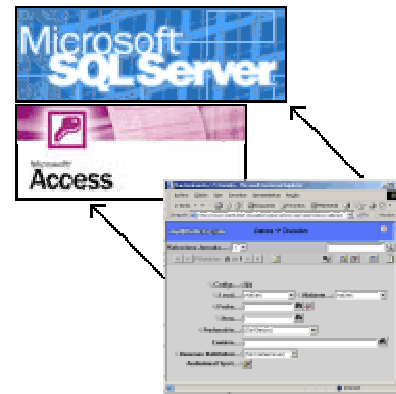




Un sistema de bases de datos; es un sistema computarizado de información para el manejo de datos por medio de software **Access** podrá hacer uso de las aplicaciones de Microsoft Office. Explicara los conceptos básicos en que se fundamenta en los llamados sistemas de manejo de base de datos (DBMS). Los tres componentes principales de un sistema de base de datos por manejar.

1.1.1 ¿Qué es una base de datos relacional?

El enfoque relacional es sustancialmente distinto de otros enfoques en términos de sus estructuras lógicas y del modo de las operaciones de entrada / salida. En el enfoque relacional, los datos se organizan en tablas llamadas relaciones, en cada una de las clases se implanta como un archivo.



En terminología relacionar una sigla es una relación que se llama ADA, representa un registro o una entidad; cada columna en una relación representa un campo o un



atributo. Así, como una relación se compone de una colección de entidades (o registros) cuyas propiedades están descritos por cierto numero de atributos predeterminados implantados como campos. En otras palabras, es un modelo relacional de base de datos que se compone de relaciones, y las relaciones entre ellas se establecen implícitamente vía claves externas.

Una de las características del enfoque relacional es la simplicidad de su representación lógica; para los usuarios es más fácil entender las tablas que los complejos árboles o estructura de una red. En un modelo relacional una tabla es una entidad separada que no ocupa un nivel jerárquico fijo. Consecutivamente se puede acceder directamente a cualquier registro en un archivo relacional sin necesidad de navegar en una red de varios niveles desde la raíz, como se requiere los niveles jerárquicos o de redes. Esta rectitud de enfoque da por resultado el acceso a los datos sin depender de la trayectoria así como una mayor independencia de los mismos.

Aunque desde el punto de vista del usuario el enfoque relacional parece más sencillo, su implantación puede ser bastante compleja. Las características relacionales se alcanzan vía un software sofisticado que requiere el tiempo extra del CPU para su ejecución como consecuencia, una de los retos más importante era alcanzar un mejor nivel de desempeño, en especial para las grandes bases de datos. Finalmente los puntos relacionales del manejo administrativo de base de datos se comercializaron a principios de los ochentas después de una década de investigación y desarrollo. Los siguientes son algunos de los sistemas relacionales actuales y los sistemas operativos que los respaldan



DEBS Relacionales	Sistemas Operativos
QUERY-BY-EXAMPLE de IBM SQL/DS de IBM DB2 de IBM INGRES de Relational Technology ORACLE de Relational Software DBASE III d SQLServer 7.0 e Ashton Tate , Oracle RDBMS 11.6 MB SQL*PLUS 1.6 MB SQL*FORMS 2.4 MB SQL*MENU 1.8 MB SQL*REPOT WRITER 2.1 MB Pro*C, Pro*Fortran, Pro*Cobol 1.3 MB NLS 2.1 MB SQL*Net 2.8 MB Oracle Demo Database <u>5.9 MB</u> SQLServer , SQLServer 7.0 Windows NT Server	VM de IBM DOS/VSE, VM/CMS de IBM MVS de IBM VMS, UNIX RSX, VMS, UNIX de DEC MS-DOS, microcomputadoras OS/2, UNIX, LINUX WINDOWS XP, MINIX, QNX CYGWIN

Se espera que los sistemas relacionales aumenten de popularidad cuando se dispongan de mejores interfases físicos-lógicas para mejorar su desempeño. Aunque las distintas implantaciones relacionales tienen características y posibilidades diferentes.

1.1.2 ¿Qué es un campo, un registro y una tabla?

Un CAMPO es la unidad más pequeña a la cual una puede referirse en un programa de computadora.



REPRESENTACIÓN DE LOS CAMPOS.

En los sistemas comunes de almacenamiento, los elementos de datos (CAMPOS) se guardan; en campos de longitud fija y con un orden predeterminado, de tal forma que el programador puede conocer el contenido de cada campo al referirse al número de carácter predeterminado del registro. Sin embargo, en los sistemas de manejo de bases de datos se utilizan disposiciones más sofisticadas. Existen cuatro formas diferentes de representar los campos:

1. La posiciona los datos de un registro se almacenan en campos consecutivos de longitud fija en un orden predeterminado. Esta disposición es sencilla de realizar y conveniente de recuperar la información guardada no utiliza todo el espacio definido, quedando este vacío.
2. La Relacional. Esta técnica elimina los espacios desperdiciados mediante el uso de un delimitador que indica el final de un campo. El delimitador debe ser un carácter especial que no se usara en ningún otro sitio en la base de datos.
3. La indexada. Se utilizaran aquí señaladores para indicar el principio de cada campo en un registro almacenado. El señalador puede ser una dirección absoluta o reactiva.
4. La Etiquetada. Cuando un archivo tiene muchos valores por omisión, puede usar, la etiquetada para almacenar únicamente los valores referentes por los omitidos.

El balance en el diseño de la representación de los campos se encuentra en la cantidad de espacio de almacenamiento y la velocidad de recuperación por lo que la elección para el diseño deberá hacerse considerando estos dos parámetros. Ninguna de las disposiciones anteriores es superior a todas las otras si consideramos ambos parámetros por ejemplo, la técnica posicional es la más sencilla pero no es buena en cuanto a la economía del espacio de almacenamiento. El método relacional reduce ese problema, por con ello disminuye la velocidad de recuperación, ya que la



información debe buscarse pasando por los datos del registro y contando con cierto numero de limitadores para encontrar finalmente la localización del campo deseado. Con la técnica Indexada se mejora la velocidad de recuperación a costa de la necesidad de mantener arreglos de señaladores.

Un conjunto de campos con relación entre si se agrupan como un REGISTRO. Una colección de registros del mismo tipo se llama ARCHIVO.

REGISTROS LÓGICOS Y REGISTROS FISICOS

- Un registro lógico representa la percepción del programador de lo que es un registro de datos para el programador, los registros lógicos en un archivo están organizados uno de tras de otro, sin importar su verdadera disposición en el dispositivo de almacenamiento.
- Un registro físico puede consistir de varios registros lógicos además de un control del sistema donde guarde información sobre el almacenamiento de datos para facilitar la búsqueda. Esta parte se llama información sobre el sistema. Un registro físico es una unidad de transferencia de datos entre el dispositivo de almacenamiento de datos y la memoria principal.

FORMAS DE REGISTRO.

Los registros lógicos representan la percepción del programador de datos contenidos en un archivo. Se han usado varios formatos de registro de distintos sistemas de computadoras para facilitar la programación. Un programador puede especificar cualquiera de los formatos disponibles en el sistema cuando se crea algún archivo.

Existen cinco tipos principales de registros de organización:

1. LONGITUD FIJA, DESBLOQUEADA.- Todos los registros dentro del archivo tienen la misma longitud y cada bloque (o registro) contiene un registro lógico.
2. LONGITUD FIJA, BLOQUEADA.- todos los registros dentro del archivo tiene la misma longitud. Cada bloque contiene varios registros; Todos los bloques en el archivo tienen la misma longitud tal como él programador los definió.



3. LONGITUD VARIABLE, DESBLOQUEADA.- los registros en el archivo son de longitud variable. La longitud del registro (LR) se almacena en un campo de 4 bytes antes del registro lógico, y es igual a la longitud de un registro lógico más 4. La longitud de bloque (LB) se guarda en un campo de 4 bytes, indicando el número de bytes en el bloque incluyéndose a sí mismo. La disposición del área de datos es como sigue: LB, LR, Registro, LB, LR, Registro...
4. LONGITUD VARIABLE, BLOQUEDO.- Este tipo de formato es similar formato de longitud variable desbloqueada, excepto que cada bloque contiene varios registros de longitud variable. El área de datos consiste en lo siguiente: LB, LR, Registro, LR, Registro, LR, Registro, LB, LR Registro...
5. INDEFINIDOS.- este tipo de formatos se usa cuando el formato de registros de algún archivo no corresponde a ninguno de los formatos de registro definidos en el sistema.

Una tabla también puede considerarse un conjunto de tuples. Si la tabla tiene “n” columnas será n-tuples y se dice que su relación es de grado n (binarias, terciarias, etc.) por su parte, cada columna constituye un dominio.

Es posible crear tablas de menor grado para los subconjuntos de interés del usuario.

1.1.3 ¿Qué es un Query?

Es una base de datos relacional, no especificas la ruta de acceso de las tablas, y no necesitas saber como los datos son arreglados físicamente.

Para acceder a la base de datos, ejecutas una estructura de lenguaje de búsqueda (structured query lenguaje) el cual es según el Instituto de Estándares Nacional Americano (SQL). El lenguaje para operaciones de una base de datos relacional. El lenguaje contiene un largo set de operadores para particionar y



combinar relaciones. La base de datos puede ser modificada usando los estándares los del SQL.

1.1.4 ¿Cómo instalar una Base de Datos?

Los programas de bases de datos más populares han sido los de DBASE: DBASE II, III PLUS y IV. Entre los dos últimos existen muy pocas diferencias,

salvo en cuanto a capacidad de almacenamiento de información.



En adelante vamos a suponer que estamos cargando DBASE III PLUS, el cual disponemos en disco flexible. Los pasos a

seguir serían:

- Estando en la unidad C: teclea A: y teclear enter,
- Estando ya en A, dar la instrucción: DBASE enter,
- Al iniciar el programa aparece una leyenda comercial, dar enter,
- Inmediatamente aparece el asistente del programa y podemos ir seleccionando en el menú el renglón que nos interesa.

1.1.5 Creación de una Tabla

La tabla puede crearse de dos formas: a través del asistente, ya identificado, o mediante el punto indicativo.

Para diseñar la base se requiere:

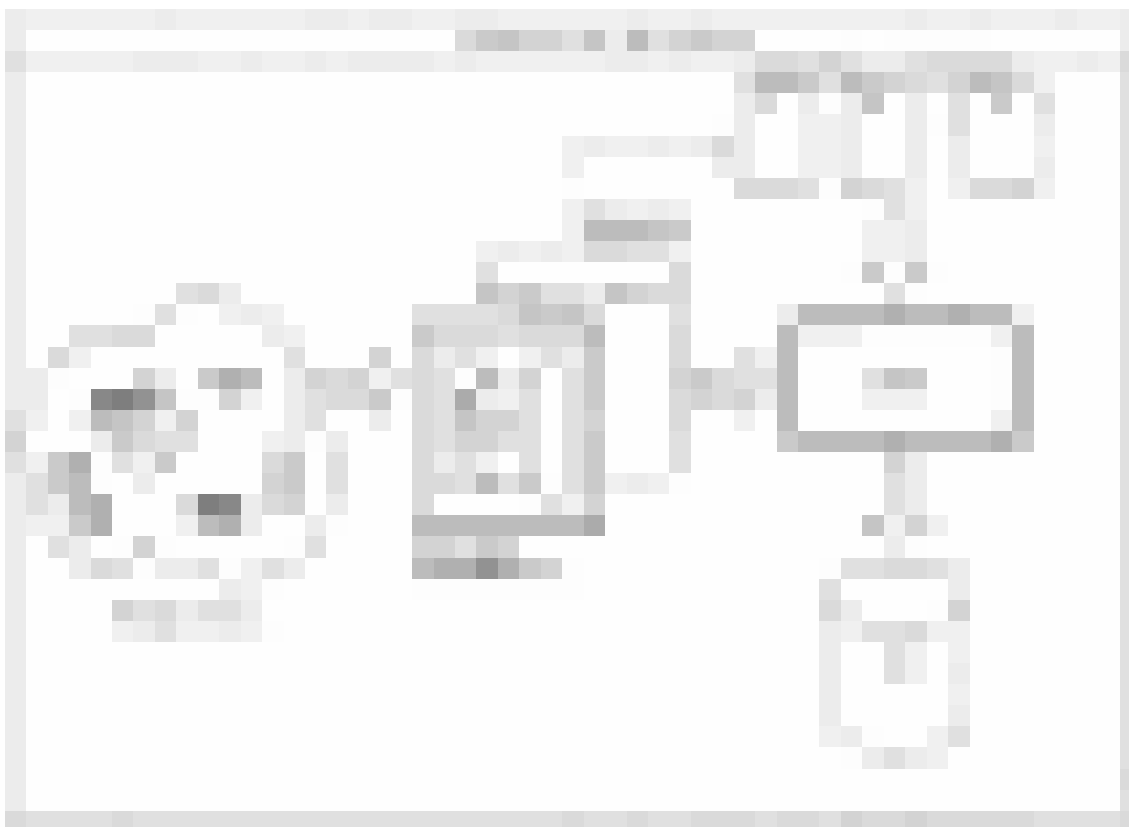
- Definición sobre la base del análisis de los datos existente.



- Refinamiento de los datos
- Establecimiento de relación entre los atributos incluidos.

Para el primer paso se recomienda hacer en papel una lista de todos los atributos importantes con los que queremos contar (ejemplo: nombre, domicilio, teléfono, etc.)

El refinamiento implica revisar la lista anterior con el objeto de ver si alguno de los atributos debe desglosarse en varios (ejemplo: apellido paterno, materno y nombre de pila en lugar de simplemente nombre como habíamos anotado antes). Esto nos lleva a tener que considerar también la cantidad y número de espacios que cada atributo ocupara en la base de datos (ejemplo: número de caracteres que conformaran la longitud del campo). En cuanto al establecimiento de relaciones se requiere determinar cuáles de ellas son las realmente importantes con base en el uso que queremos hacer de la misma.





Diseñada la base se procede a cargarla. Suponiendo que usamos el punto indicativo procederemos como sigue:

- Para dejar el ayudante y pasar al punto indicativo, presionar ESC. El punto aparece al final de la pantalla, indica que esta en modo interactivo, por lo que podemos darle ordenes.
- La primera orden implica decirle en que unidad guardara la base de datos. Por ejemplo: en el mismo disco en que esta trabajando. La instrucción será entonces:
.SET DEFAÚLT TO A, enter
- Si por el contrario queremos guardar la información en disco duro, será:
.SET DEFAÚLT TO C, enter.
- La segunda orden, estando en el punto indicativo, corresponde a teclear:
.CREATE, enter.
- El programa nos pedirá el nombre del archivo, lo introducimos teniendo en cuenta que no debe exceder de 8 caracteres y que debe comenzar con una letra.
El asignara automáticamente la extensión: DBF.
- DBASE desplegara una pantalla con bloques resaltados para introducir los nombres de los campos, sus tipos, longitudes y un numero de dígitos decimales.
- Para nombrar un campo debe seleccionarse una palabra que lo describa lo mejor posible, pueden constar de hasta 10caracteres y constituirse por letras,
- Numero o subrayados, pero deben comenzar con una letra.
- Después de poner el nombre se pulsa enter y el cursor se desplaza
- Automáticamente al siguiente bloque: tipo de campo.
- Los campos pueden ser:



- Campo, carácter / texto: guarda caracteres como letras, números, símbolos o espacios en blanco.
- Campo de fecha en formato MM / DD /AA. Las barras // las introduce automáticamente.
- Campos numéricos, con o sin decimales.
- Como lógicos, como verdadero donde se usan letras Y o T, y falso en que se emplean F o M.
- Campo memo, para guardar grandes bloqueos de texto

Definido el campo apropiado a nuestra necesidad, se pasa a la longitud del campo.

- Se define el número de caracteres que se empleará en cada registro: ejemplo: en el primero 12 y enter, en el segundo 15 y enter, en el tercero.....
- Luego se define de igual manera el número de decimales a emplear, en aquellos casos en que el tipo se haya definido como numérico.
- Al finalizar se pulsa dos veces la tecla enter y el sistema estará listo para comenzar a introducir los datos.

1.1.6 Elaboración e Impresión de Reportes.

Una vez introducidos todos los registros podemos desde el punto indicativo dar la orden de LIST y DISPLAY para examinar el contenido de nuestra base de datos.



Si solo queremos que nos muestre algunos campos se anota su nombre a continuación de la orden LIST. Si varios se separan con comas. Con DISPLAY puedo pedirle que me muestre determinada información. Ejemplo: Si le doy la instrucción: GO 5, Enter, seguida de DISPLAY



RECORD, se mostrara el contenido del registro N°5.

Si le escribo: GO 5, Enter, seguida de DISPLAY NEXT 2, enter, ira al registro N°5 y se mostrara dos registros: este y el siguiente.

Para imprimir la BASE de DATOS se da, desde el punto indicativo, la instrucción: LIST TO PRINT, Enter.

Para salir del programa se utiliza QUIT desde el punto indicativo.

Para generar un informe se usa CREATE REPORT.




MANEJO BASICO DE LAS BASES DE DATOS

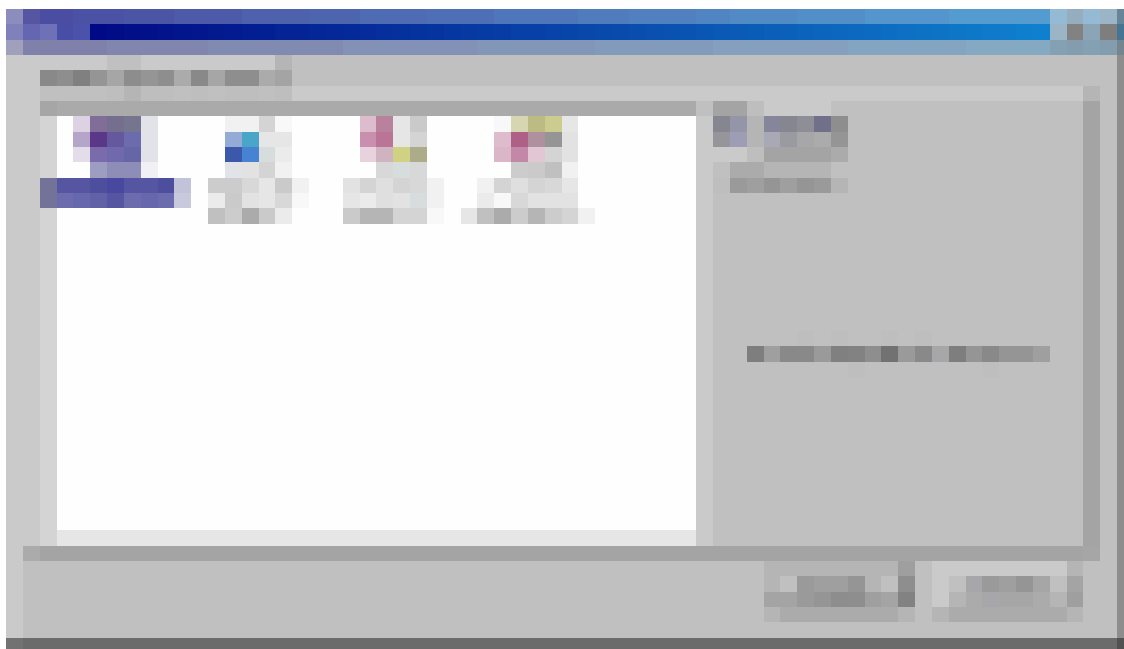
Cuando creamos una base de dato, aparece una ventana cuyo trabajo es ofrecer de manera cómoda y sencilla operaciones mas comunes que puedan llevarse a cabo en una base de datos.

Para obtener este cuadro es necesario crear una nueva base de datos que contendrá todas esas operaciones comunes, así como las tablas que componen la base.



CREACIÓN DE BASES DE DATOS

Vamos a empezar por indicar la forma en que se crea una base de datos. El proceso es realmente simple. Podemos elegir la opción **Nueva base de datos** en el menú Archivo, pulsar las teclas **CONTROL + U**, o bien pulsar el botón  de la barra de herramientas de Access en cualquiera de los tres casos obtendremos lo siguiente:



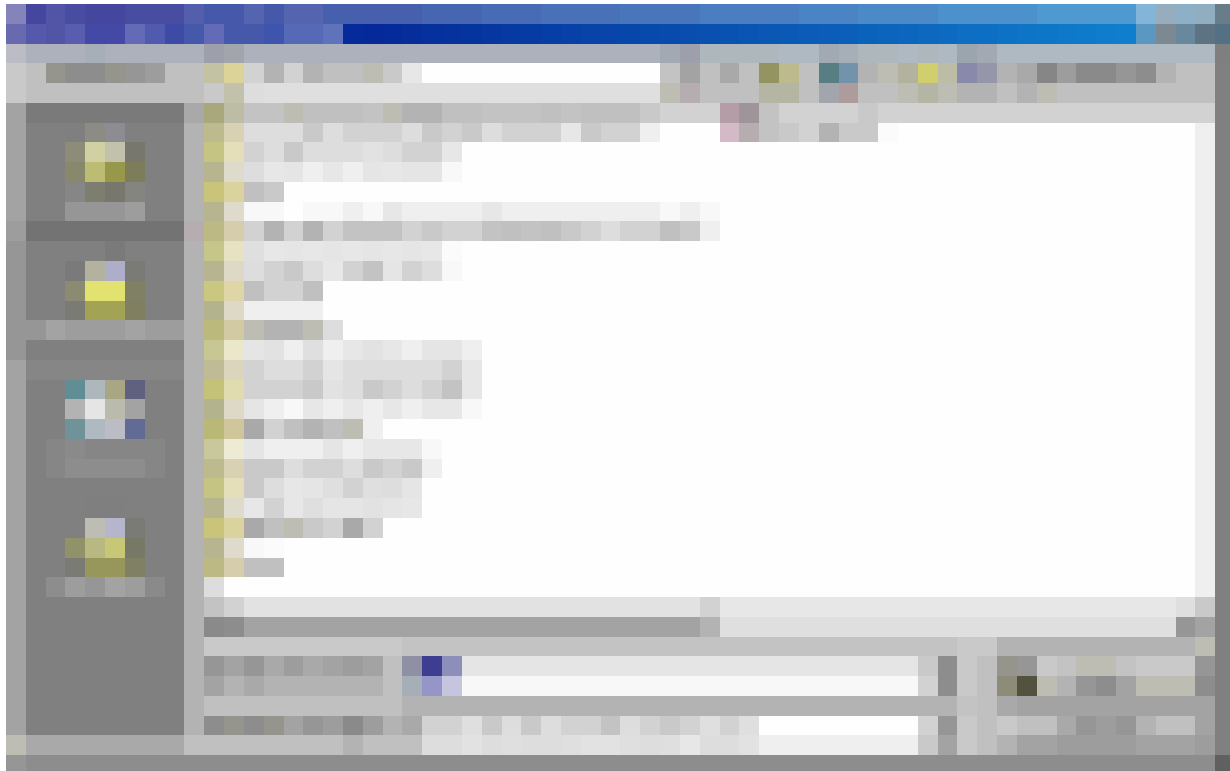
Como vemos, hay dos fichas que podemos seleccionar:

1. **General:** cuyo único contenido hasta el momento es el icono **Base de datos en blanco**. Activar ese icono supone la creación de una base de datos en la que no hay absolutamente nada definido.
2. **Base de datos:** Esta ficha contiene varias bases de datos predefinidas por Microsoft en las que solo será necesario rellenar los datos puesto que la estructura de la base que se seleccione ya estará creada.



Por ejemplo, si se desea crear una base de datos sobre nuestras películas de videos podríamos elegir el icono **Colección de videos** que muestra la citada ficha **Bases de datos**.

A continuación, Access muestra un cuadro de dialogo en el que debemos dar nombre a la nueva base de datos, entre otras cosas. Este es el cuadro:



1. lo primero que Access requiere para crear un nueva base de datos es el nombre con el que quedara gravado en el disco como un archivo mas. Por tanto, utilizaremos el campo **Nombre de archivo** para escribirlo. En la lista que aparece podemos elegir un nombre. Si así lo hacemos, Access almacenara la nueva base de datos sobre aquella que tenia antes ese nombre, borrándola, y pidiendo primero confirmación para la acción.
2. Otra posibilidad es elegir el lugar en el que se almacenara la base de datos. Para ello utilizaremos la lista **Guardar en**, que nos ofrece una relación con

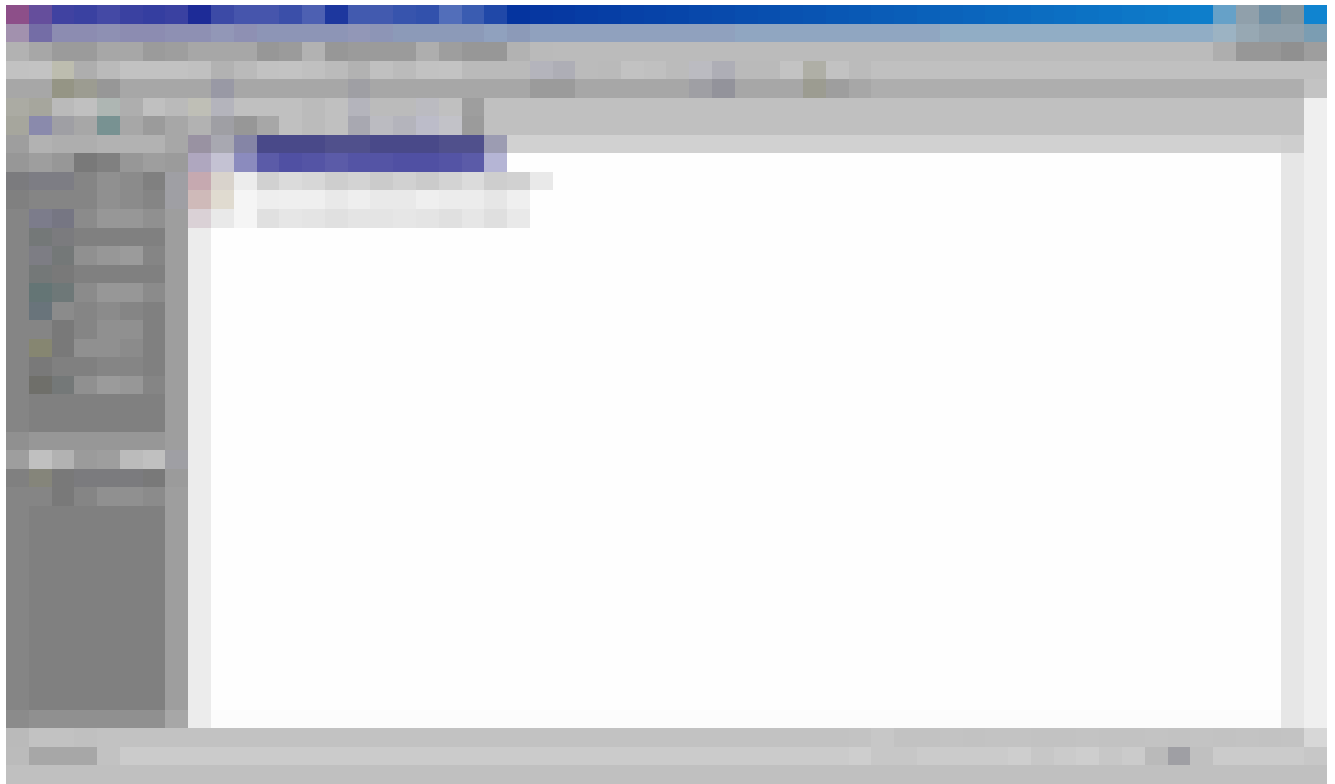


todas las unidades de disco del sistema. Cuando se elige una unidad de disco aparecen todas sus carpetas y archivos en cuadro central.

3. utilice la lista **Guardar como tipo** para establecer que clase de base de datos deseamos crear. Lo normal es que aparezcan las bases de datos de Access.
4. El botón de revisión Exclusivo se muestra disponible solo en entornos multiusuario (redes). Si una base de datos se abre de forma exclusiva, ningún otro miembro de la red puede abrirla si antes no la cierra aquel que la haya abierto de modo exclusivo. Esto evita problemas al disco, ya que si dos usuarios de una red pudieran abrir una base de datos al mismo tiempo, al intentar añadir datos (registros) o al modificar alguno que ya exista, se podría entrar en conflicto, porque el ordenador no “sabría” a cual de los dos usuarios de la red hacer caso. No obstante, Access le permite abrir una base de datos en modo compartido de modo que cualquier usuario de la red tenga acceso a la base. El problema esta en que los datos que queden definitivamente almacenados serán los del ultimo usuario que los almacene en el disco. Existe una serie de privilegios que pueden asignarse a usuarios de la red. Por ejemplo, se puede asignar a un usuario unidamente la capacidad de leer una base de datos, con lo cual tendrá restringido el acceso para cualquier otra operación, como, por ejemplo, gravar los datos que incorpore a la base.
5. Cuando haya elegido todos los datos para la nueva base, pulsa el botón

Aceptar

Una ves que ha hecho esto Access crea la base de datos y muestra una ventana que contiene todos sus elementos hasta ahora vacíos. Este ventana recibe el nombre de Ventana de base de datos y su aspecto, vacío, es este:



LA VENTANA DE BASE DE DATOS

La ventana de base de datos muestra como menú un grupo de fichas con las operaciones posibles dentro de una base de datos. Al elegir una ficha, obtenemos cuantos elementos de ese tipo contiene la base de datos.

Como hemos visto en la figura, en la ventana de base de datos existen varias fichas.

1. **Tablas:** ya hemos comentado algo de las tablas y veremos mas adelante datos nuevos sobre ellas, se puede decir que las tablas son los cimientos sobre los que se construye la base de datos ya que estas contienen los datos que utilizaremos para trabajar con el resto de las funciones.
2. **Consultas;** las consultas son cuestiones que se plantean en las bases de datos para obtener ciertos resultados, normalmente mediante un ejemplo. Generalmente, las consulta generan un listado con el resultado de la cuestión que se ha planteado sobre una base de datos. Por ejemplo, podríamos




consultar cuantos individuos de una tabla son mayores de edad y access generaría una lista de aquellos que cumplen esa condición. El resultado siempre es una tabla que contiene los datos consultados, con la ventaja añadida de que si se modifican los datos de la tabla desde la que se ha creado la consulta esta también resulta actualizada.

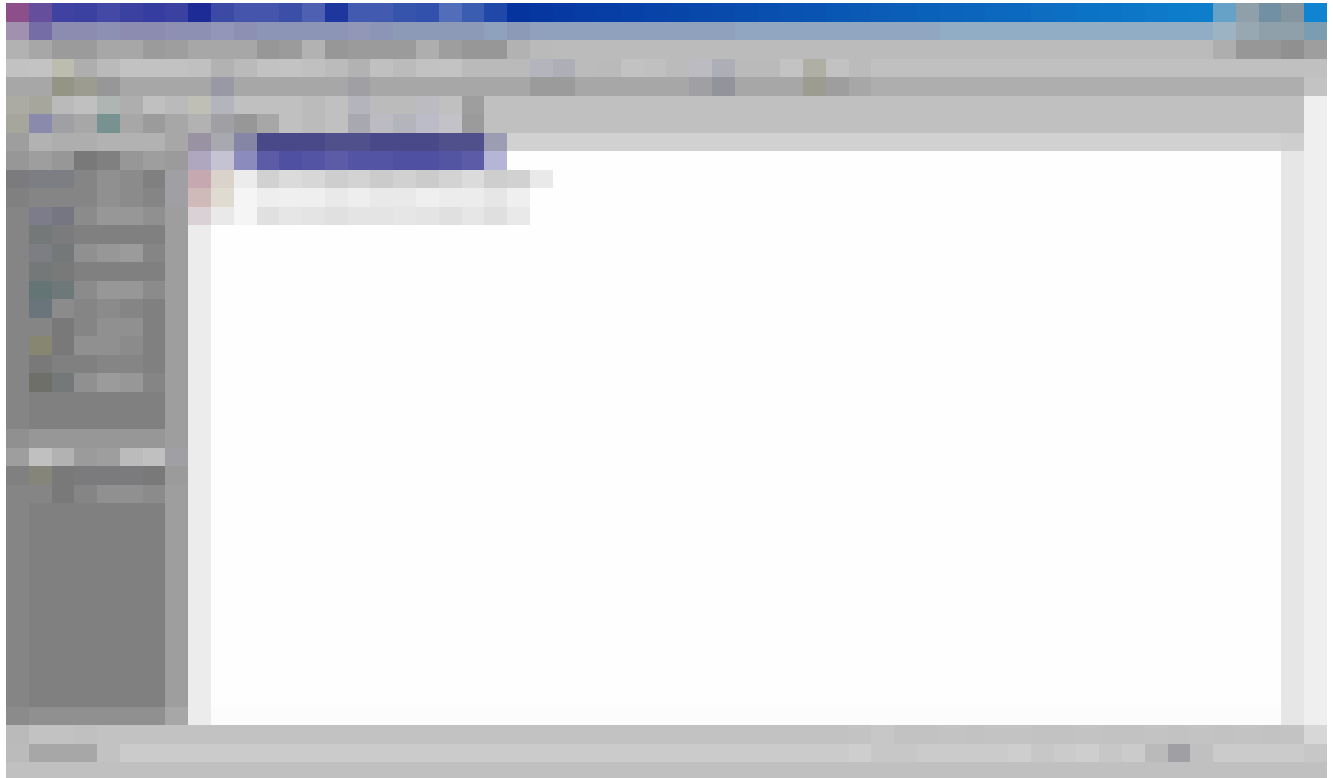
3. **Formularios.** Son plantillas cuya finalidad es ser modelado de los datos de una base. El resultado de la creación de un formulario es que access permitirá introducir y editar los datos de una tabla, o incluso los de la base de datos completa, de una forma mas profesional (El lugar de directamente sobre la tabla original). Su función es puramente estética y para un manejo mas cómodo, si bien su construcción, puede ser desde muy simple hasta muy compleja.
4. **Informes** he aquí otro tipo de plantilla que utiliza los formatos de la s tablas o consultas para generar un enunciado que suele ir destinado a la impresora. Los informes se informan mediante un texto común y datos extraídos de las tablas o consultas. Cada registro suele destinarse a una sola hoja, salvo en casos concretos como las etiquetas postales que reúnen varios registros en una misma pagina.
5. **Macros:** Un macro es una función compleja que se ha construido partiendo de otras mas simples. Podemos realizar macros de modo que al pulsar una tecla o seleccionar una opción de menú (por ejemplo),. Access realizara varias operaciones que usualmente realizamos a menudo de manera automática.
6. **Módulos.** Un modula es una parte de un programa realizado con un lenguaje de programación que proporciona access. Para utilizarlo es necesario tener ciertas nociones de programación así como un profundo conocimiento del lenguaje de access.

Para seleccionar cualquiera de estas fichas, bastara con llevar el ratón hasta una de ellas y pulsar el botan izquierdo de este. Automáticamente aparece en el cuadro de la izquierda, una lista de elementos que existan sobre ese tema dentro de la base de







datos. Por ejemplo, al pulsar sobre la ficha  Tablas obtendremos todas las tablas disponibles de la base de datos activa.


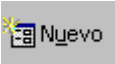

Veamos de nuevo la ventana de base de datos:



Existen en ella tres botones que aun no hemos visto:

1.  Abrir Con este botón podrá abrir elemento de cualquier ficha. Para ello seleccione una ficha cualquiera y después elija de la lista el elemento que desee. Pulse el botón  Abrir (o bien haga doble clic en el elemento) y access lo abrirá para poder trabajar en el por ejemplo, si desea abrir una tabla, Elija la ficha tabla y seleccione una tabla de las que aparezcan en la lista pulsando el botón  Abrir . Si no aparece ninguna tabla en la lista es porque en esa base de datos no existen tablas. Pulse, pues, el botón  Nuevo Si desea crear una tabla para la base de datos actual.



2.  el botón de diseño permite abrir la estructura de una elemento para modificarla. Por ejemplo, la estructura de una tabla esta formada por sus campos y los tipos. Pulse este botón para modificara la estructura, añadiendo campos para cada registro o eliminando alguno que ya tenga.
3.  Utilice este botón para crear un elemento nuevo dentro de la ficha elegida . por ejemplo, se elegí la ficha consulta, con el botón  podrá crear otra consulta a añadir a las que ya tenga.

ASITENTE DE Access

Los asistentes de Access permiten crear nuevo elemento en una base de datos definiéndolo o por pasos el objetivo principal de los asistentes es hacer fácil una tarea difícil. Para ello, Access desglosa la creación de un elemento cualquiera de una base de datos en varios pasos por los que nos guía para crear el elemento sin ningún tipo de error o de complicación final.





Unidad 2.

Concepto de telecomunicaciones, virus informáticos

2.1 Telecomunicaciones.

2.1.1 Conexión entre una computadora y sus terminales remotas.

2.1.2 Conexión punto a punto.

2.1.3 Conexión multipunto.

2.1.4 Enlaces de larga distancia.

2.1.5 Software para redes.

2.1.6 Funciones y caracterización de redes.

2.1.6.1 Redes locales.

2.1.6.2 Redes metropolitanas.

2.1.6.3 Redes amplias o globales.

2.1.7 Internet ANEXO 1 (INTERNET, EUDORA, PINE)

2.1.8 Modelo jerárquico ISO/OSI

2.2 Virus informáticos.

2.2.1 Qué son los virus informáticos.

2.2.2 Clasificación de virus informáticos.

2.2.3 Cómo funcionan los virus informáticos.

2.2.4 Cómo se eliminan los virus informáticos.

2.2.5 Medidas de seguridad.





Objetivos particulares de la unidad

Al finalizar la presente unidad reconocerás las diferentes formas en las cuales se conforma una red de Telecomunicaciones, identificando su estructura, su aplicación y los problemas de seguridad con ataques de virus, trojanos, spyware y demás malware, y podrás resolver situaciones derivadas de éste tipo de ataques.





2.1 Telecomunicaciones.

Los primeros ordenadores disponibles comercialmente resultaban demasiado primitivos para permitir las comunicaciones. La evolución de la tecnología y las mejoras del software permitieron aumentar las prestaciones de los equipos. Se mejoraron los dispositivos de almacenamiento y se desarrollaron sistemas operativos capaces de soportar varias tareas en tiempo compartido. De esta forma, podían mantenerse varias tareas del sistema activas mientras se atendía a otros usuarios de forma interactiva.



La década de los sesenta resultó de capital importancia para el desarrollo de la Telemática. Los trabajos llevados a cabo por la Agencia de Investigación de Proyectos Avanzados (ARPA) configuraron un primer modelo de sistema teleinformático, que heredaba de los sistemas telefónicos la idea de una red de comunicaciones, proveedora de servicios a una serie de centros usuarios.

Desde 1970 asistimos a un espectacular crecimiento de las redes. Aparecieron arquitecturas concebidas para sistemas distribuidos: SNA de IBM (1974), DNA de Digital (1976) etc. Este gran desarrollo trajo como consecuencia la necesidad del establecimiento de estándares que hicieran posible la comunicación entre sistemas producidos por distintos fabricantes, lo que conduce a los denominados sistemas abiertos.

En 1977 el comité técnico número 97 (TC-97) de la Oficina Internacional de Estándares ISO creó un nuevo subcomité (SC-16) encargado de resolver esta situación de carencia de una filosofía y estructura de comunicaciones común. El



objetivo de este subcomité fue el establecimiento de una arquitectura que proporcionara el marco de definición. El desarrollo y la validación de estándares en la nueva generación de sistemas de información distribuida.

A través de este texto, utilizaremos el concepto de redes de ordenadores para dar a entender una colección *interconectada* de ordenadores *autónomos*. Se dice que dos ordenadores están interconectados, si estos son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre también puede hacerse mediante el uso de láser, microondas y satélites de comunicaciones. Al indicar que los ordenadores son autónomos, queremos excluir de nuestra definición a los sistemas en donde existe una clara relación maestro/esclavo. Si un ordenador puede forzosamente arrancar, parar o controlar a otro, éstos no se



consideran autónomos. Un sistema constituido por una unidad de control y muchos esclavos no es una red, ni tampoco lo es un ordenador grande con lectoras de tarjetas de control remoto, impresoras y terminales.

Existe en la literatura una notable confusión entre una red de ordenadores y un sistema distribuido. La clave de la diferencia es que en un sistema distribuido la existencia de múltiples ordenadores autónomos es transparente al usuario (es decir, no le es visible). Él puede teclear un comando para correr un programa, y observar que corre. El hecho de seleccionar el mejor procesador, encontrar y transportar todos los archivos de entrada al procesador y poner los resultados en el lugar apropiado, depende del sistema operativo.

En otras palabras, el usuario de un sistema distribuido no tiene conocimiento de que hay múltiples procesadores, más bien se ve al sistema como un mono-procesador virtual. La asignación de trabajos al procesador y archivos a discos, el movimiento de



archivos entre donde se almacenan y donde son necesarios, y todas las demás operaciones del sistema, deben ser automáticas.

Con una red, el usuario debe *explícitamente* entrar en una máquina, *explícitamente* enviar trabajos remotos, *explícitamente* mover archivos y, por lo general, gestionar de manera personal toda la administración de la red. Con un sistema distribuido nada se tiene que hacer de forma explícita, todo lo hace de manera automática el sistema sin que el usuario tenga conocimiento de ello.

Un sistema distribuido es efectivamente un caso especial de una red, aquél cuyo software da un alto grado de cohesión y transparencia. Por lo tanto, la diferencia entre una red y un sistema distribuido está más bien en el software (en especial el sistema operativo) que en el hardware.

2.1.1 Conexión entre una computadora y sus terminales remotas.

Una de las primeras y más importantes redes abiertas es la Arpanet (USA). Su nombre viene de *Advanced Research Projects Agency*, que pertenece al DOD o *Department of Defense*. A finales de los años 60 esta red conectaba los departamentos de ciencias de varias universidades y algunas empresas privadas. Actualmente cubre medio globo terrestre, desde Hawaii hasta Noruega. Mucho del presente conocimiento sobre redes es consecuencia directa del proyecto *Arpanet*.

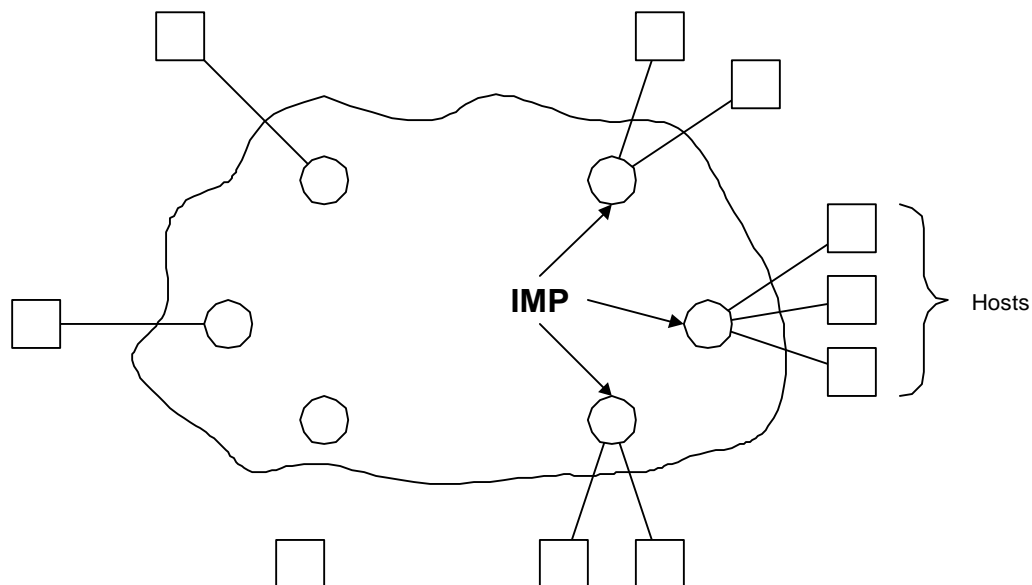
Arpanet diferencia en una red los siguientes elementos:

Host: Máquinas que ejecutan procesos de usuario (aplicaciones). En esta definición se incluyen los mecanismos de acceso a la sub-red.

Sub-Red: Mecanismos que permiten el paso de información de un host a otro. En la mayor parte de las redes de área extendida, una sub-red consiste de dos componentes diferentes: las líneas de transmisión y los IMP:



- 1 **Líneas de transmisión;** también se denominan circuitos o canales. Es el medio físico a través del cual se realiza la transmisión de los datos.
- 2 **I.M.P. (Interface Message processor):** también llamados nodos, conmutadores de paquetes, ordenadores de comunicaciones, intercambiadores de datos, sistemas intermedios, etc. Son ordenadores especializados que sólo ejecutan programas de comunicaciones. Su misión es habilitar una conexión entre en dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación deberá seleccionar una línea de salida para reexpedirlos.



Relación entre hosts e IMPs

En términos generales, puede decirse que hay dos tipos de diseños para la sub-red de comunicación:

Canales **punto a punto** (point to point).

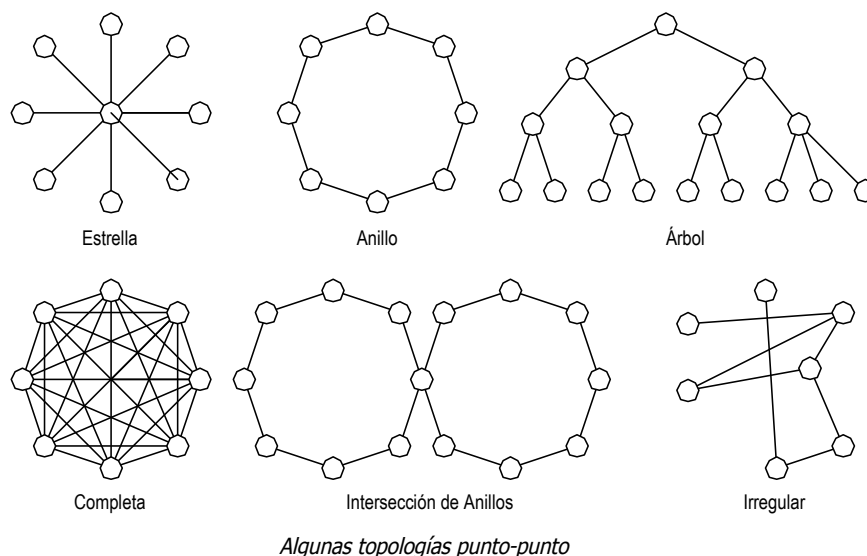
Canales de difusión o **multipunto** (broadcast).



2.1.2 Conexión punto a punto.

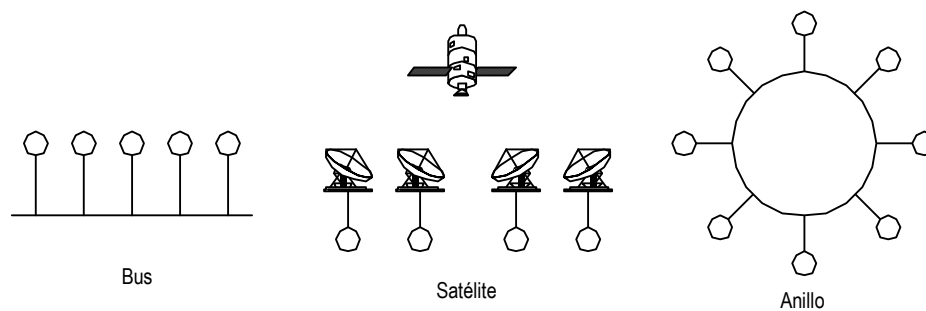
En el primero de ellos, la red contiene varios cables o líneas telefónicas alquiladas, conectando cada una de ellas un par de IMP. Si dos IMP desean comunicarse y no comparten un cable común, deberán hacerlo indirectamente a través de otros IMP. Cuando un mensaje (que en el contexto de sub-red normalmente se denomina paquete o packet) se envía de un IMP a otro, a través de uno o más IMP intermediarios, el paquete se recibe íntegramente en cada uno de estos IMP intermediarios. Se almacenará ahí y no continuará su camino hasta que la línea de salida necesaria para reexpedirlo esté libre. La sub-red que utiliza este principio se denomina sub-red punto a punto, de almacenamiento y reenvío o de conmutación de paquetes. Casi todas las redes de área extendida tienen sub-redes del tipo de almacenamiento y reenvío.

Un aspecto importante de diseño, cuando se utiliza una sub-red punto a punto, consiste en considerar cómo deberá ser la topología de interconexión de los IMP. En las redes locales que se diseñaron como tales, tienen por lo general una topología simétrica. A diferencia de éstas, las redes de área extendida tienen típicamente topologías irregulares.



2.1.3 Conexión multipunto.

La estructura multipunto se emplea como un segundo tipo de arquitectura de comunicación y la utilizan la mayoría de las redes de área local y un número muy reducido de redes de área extendida. En una red de área local, el IMP se reduce a un solo chip, el cual se incluye en el interior del host, de tal manera que siempre habrá un host para cada IMP, mientras que en una red de área extendida podrá tener varios hosts por IMP.



Comunicación de subredes de difusión

Los sistemas multipunto (o de difusión) tienen un solo canal de comunicación que, a su vez, es compartido por todas las máquinas que constituyen la red. Los paquetes que una máquina cualquiera envía, son recibidos por todas las demás. El campo de dirección, localizado en el interior de un paquete, especifica a quién va dirigido. En el



momento en que se recibe un paquete, se verifica el campo de dirección y, si el paquete está destinado a otra máquina, éste simplemente se ignora. En cualquier instante, una máquina conectada a una sub-red multipunto, tiene la función de maestra y está capacitada para transmitir. El resto de las máquinas no pueden enviar. Se necesita un mecanismo de arbitraje para resolver los conflictos en el momento en que dos o más máquinas quieren transmitir a la vez. Este mecanismo de arbitraje puede estar centralizado o distribuido. Resumiendo, podemos dividir las topologías multipunto en:

Estáticas: Cada IMP posee el canal para transmitir durante un tiempo predeterminado (*Quantum*), que se desperdicia en caso de que el IMP no tenga nada que transmitir.

Dinámicas: Dentro de las cuales existen dos tipos:

- *Centralizadas:* Un IMP que desea transmitir lo solicita a un elemento común que arbitra.
- *Descentralizadas:* Los IMP deciden por sí mismos si pueden o no tomar el canal para transmitir.

2.1.4 Enlaces de larga distancia.

Uno de los desarrollos más sorprendentes de los últimos años es indudablemente la posibilidad de conectar todas las redes de cobertura limitada en una red global que, al menos en teoría, permite enlazar y comunicar usuarios ubicados en cualquier parte del mundo. Esto es lo que ha dado origen a términos como globalización de la información. Actualmente existen redes de telecomunicaciones que permiten comunicación telefónica instantánea entre





dos usuarios de dos países del planeta, que envían información financiera entre instituciones de dos países cualesquiera, que envían señales de televisión de un país a otro, o que permiten localizar personas por medio de receptores de radio en muchos países del mundo.

2.1.6 Funciones y caracterización de redes.

Puesto en una forma más general, el tema aquí consiste en compartir recursos, y el objetivo es hacer que todos los programas, datos y equipos estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000km de distancia de los datos, no debe evitar que éste los pueda utilizar como si fueran originados localmente. Otro aspecto de compartir recursos es el relacionado con la distribución de la carga.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo, todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible (como consecuencia de un fallo de hardware), podría utilizarse alguna de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico. Los ordenadores pequeños tienen una mejor relación costo/rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor.



Otro objetivo del establecimiento de una red de ordenadores no tiene nada que ver con la tecnología. Una red de ordenadores puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre si.

Distancia entre procesadores	Procesadores ubicados en el mismo...	Ejemplo
0,1m	La tarjeta del circuito	Máquina de flujo de datos
1m	El sistema	Multiprocesador
10m	El cuarto	Red Local
100m	El edificio	"
1Km	La ciudad	Red de gran alcance
100Km	El país	"
1000Km	El continente	Interconexión de redes de gran alcance
10,000Km	El planeta	"

En la tabla anterior, se muestra la clasificación de sistemas multiprocesadores distribuidos de acuerdo con su tamaño físico. En la parte superior se encuentran las máquinas de flujo de datos, que son ordenadores con un alto nivel de paralelismo y muchas unidades funcionales trabajando en el mismo programa. Después vienen los multiprocesadores, que son sistemas que se comunican a través de memoria compartida. Enseguida de los multiprocesadores se muestran las verdaderas redes, que son ordenadores que se comunican por medio del intercambio de mensajes. Finalmente, a la conexión de dos más redes se le denomina interconexión de redes.

Para una comunicación entre dos estaciones se precisa de una conexión física entre ambas. Esta conexión puede tener lugar con diferentes tipos de medios, tanto guiados como no guiados. En el caso de los medios guiados su aspecto más frecuente es el de un cable.





Cuando se desea interconectar a una comunidad de usuarios numerosa, una primera opción es la interconexión total, es decir, la conexión de todos con todos, de ésta forma es posible la comunicación entre cualquier pareja de usuarios. Sin embargo, esta opción es impensable en general, debido a su alto coste y al poco aprovechamiento de recursos que supone.

Como opción alternativa, se plantea el desplazar el problema a un sistema que se encargue de la interconexión y que recibe el nombre de red comunicación (que en el caso de interconexión de ordenadores se particulariza a red de ordenadores). El objetivo de esta red es facilitar la comunicación entre cualquier pareja de estaciones.

La interconexión a la red se produce ahora sobre la base de una conexión (un cable) que enlaza a cada usuario con la red de comunicación lo que permite la comunicación desde o hasta la red, generalmente suele tratarse de un enlace punto a punto dedicado. Y, en segundo lugar existe una serie de interconexiones dentro de la red que facilitan la comunicación de las estaciones.

Habitualmente las redes están compuestas de una serie de canales de comunicación y unos elementos activos de conmutación. No se suele emplear la interconexión total (por su elevado coste), aunque suele introducirse cierta redundancia para evitar que un fallo en un enlace aisle partes de la red.

La misión de los elementos de conmutación, denominados nodos o IMPs (*Interface Message Processor*), es conducir la información en cada bifurcación de la red hacia su destino final. A esta tarea se le denomina encaminamiento.

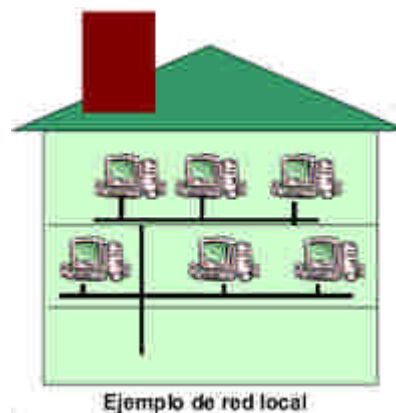
Puesto que existen más de dos estaciones conectadas a la red, es preciso que exista un esquema de selección o direccionamiento para que se pueda especificar origen y destino de la información. Cada estación debe tener una dirección que la identifique de manera única.



Todo esto conduce al concepto de redes con varios ordenadores localizados en el mismo edificio. A este tipo de red se le denomina LAN (Local Area Network) o Red de Área Local, en contraste con lo extenso de una WAN (Wide Area Network) o Red de Área Extendida.

2.1.6.1 Redes locales.

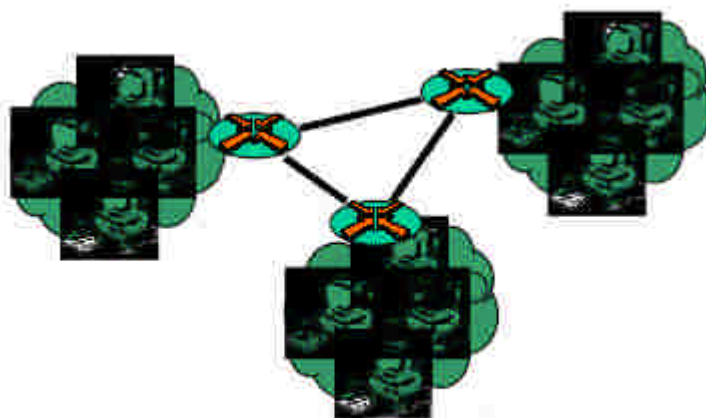
Las redes LAN son las redes de dimensiones reducidas, generalmente **decenas de metros**, como por ejemplo las constituidas por los PC's que encontramos en oficinas y domicilios. Este tipo de redes conecta un número limitado de equipos (impresoras, PC's, scanners, faxes, etc..) y la conectividad entre los elementos está asegurada a través de un mismo cableado. El protocolo más utilizado en estas redes es el Ethernet 10/100/1000 Mbit/s



Ejemplo de red local

2.1.6.2 Redes metropolitanas.

Las redes MAN se producen como extensión de LAN a las áreas geográficamente más extensas, generalmente abarcando varios kilómetros.



Estructura de una red MAN

Imaginémonos el caso de una empresa con varias sucursales en la misma ciudad. Esta empresa tendría varias LAN's en sus edificios y si estuvieran conectadas entre si

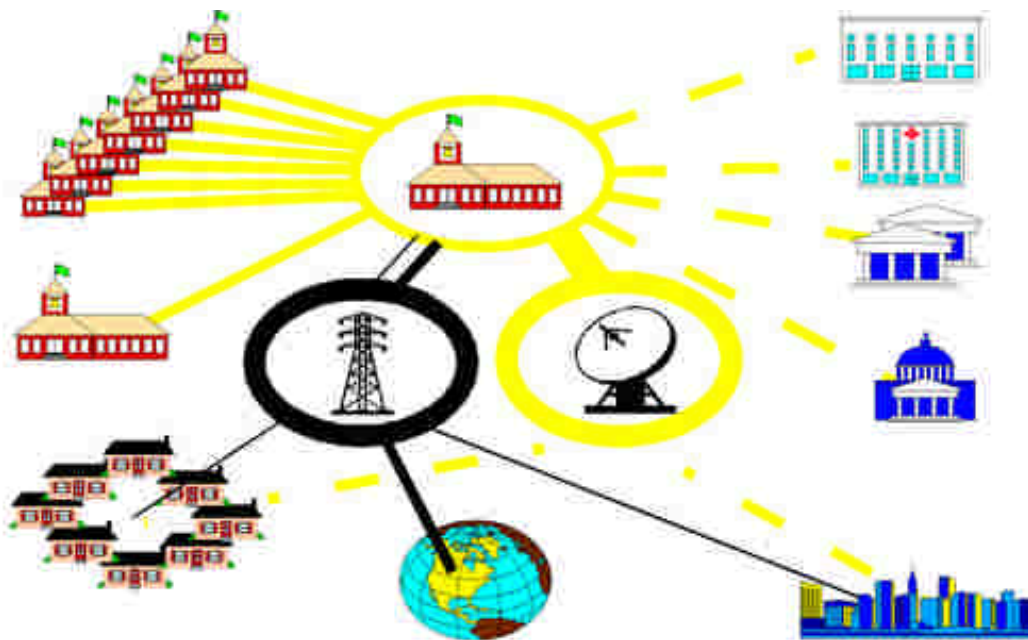
mediante líneas alquiladas y equipos que gestionaran el intercambio de información



entre las sedes, formaría en su conjunto una MAN. Los protocolos y equipos de red que se usan en las MAN están adaptados para trabajar con un número de equipos y una capacidad de transmisión por equipos muy superiores a las redes de área local. El protocolo más utilizado en este tipo de redes es FDDI (f.o.), Token Ring (F.o), X.25 y Frame Relay.

2.1.6.3 Redes amplias o globales.

La extensión del concepto de MAN a varias regiones o zonas geográficamente muy alejadas da origen al concepto de WAN o red distribuida. Los protocolos más utilizados para estas redes son TCP/IP, ATM y Frame Relay.





2.1.7 Internet

Varias redes pueden conectarse entre sí formando una red lógica de área mayor. Para que la transmisión entre todas ellas sea posible se emplean los *routers*, que son los sistemas que conectando físicamente varias redes se encargan de dirigir la información por el camino adecuado. Cuando las redes que se conectan son de diferente tipo y con protocolos distintos se hace necesario el uso de los *gateways*, los cuales además de encaminar la información también son capaces de convertir los datos de un protocolo a otro. Generalmente los términos *router* y *gateway* se emplean indistintamente para referirse de forma general a los sistemas encargados del encaminamiento de datos en Internet.

Lo que se conoce como **Internet** es en realidad una red de redes, la interconexión de otras redes independientes de manera que puedan compartir información entre ellas a lo largo de todo el planeta. Para ello es necesario el uso de un protocolo de comunicaciones común. El protocolo que proporciona la compatibilidad necesaria para la comunicación en Internet es el *TCP/IP*.



TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con *hardware* y *software* incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de *hardware*.



TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (*Transmission Control Protocol*) y el IP (*Internet Protocol*), que son los que dan nombre al conjunto. En Internet se diferencian cuatro niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- **Aplicación:** Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (*Hypertext Transfer Protocol*).
- **Transporte:** Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.
- **Internet:** Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.
- **Enlace:** Los niveles OSI correspondientes son el de enlace y el nivel físico. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada *host*, como puede ser una línea punto a punto o una red *Ethernet*.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP



es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP/IP cada una de estas unidades de información recibe el nombre de "datagrama" (*datagram*), y son conjuntos de datos que se envían como mensajes independientes.

2.1.7.1 TCP (Transmission Control Protocol).

El protocolo de control de transmisión (TCP) pertenece al nivel de transporte, siendo el encargado de dividir el mensaje original en datagramas de menor tamaño, y por lo tanto, mucho más manejables. Los datagramas serán dirigidos a través del protocolo IP de forma individual. El protocolo TCP se encarga además de añadir cierta información necesaria a cada uno de los datagramas. Esta información se añade al inicio de los datos que componen el datagrama en forma de cabecera.

La cabecera de un datagrama contiene al menos 160 bit que se encuentran repartidos en varios campos con diferente significado. Cuando la información se divide en datagramas para ser enviados, el orden en que éstos lleguen a su destino no tiene que ser el correcto. Cada uno de ellos puede llegar en cualquier momento y con cualquier orden, e incluso puede que algunos no lleguen a su destino o lleguen con información errónea. Para evitar todos estos problemas el TCP numera los datagramas antes de ser enviados, de manera que sea posible volver a unirlos en el orden adecuado. Esto permite también solicitar de nuevo el envío de los datagramas individuales que no hayan llegado o que contengan errores, sin que sea necesario volver a enviar el mensaje completo.



Formato de la cabecera TCP.

Puerto origen		Puerto destino	
Número de secuencia			
Señales de confirmación			
Tamaño	Reservado	Bits de control	Window
Checksum		Puntero a datos urgentes	

A continuación de la cabecera puede existir información opcional. En cualquier caso el tamaño de la cabecera debe ser múltiplo de 32 bits, por lo que puede ser necesario añadir un campo de tamaño variable y que contenga ceros al final para conseguir este objetivo cuando se incluyen algunas opciones. El campo de tamaño contiene la longitud total de la cabecera TCP expresada en el número de palabras de 32 bits que ocupa. Esto permite determinar el lugar donde comienzan los datos.

Dos campos incluidos en la cabecera y que son de especial importancia son los números de puerto de origen y puerto de destino. Los puertos proporcionan una manera de distinguir entre las distintas transferencias, ya que un mismo ordenador puede estar utilizando varios servicios o transferencias simultáneamente, e incluso puede que por medio de usuarios distintos. El puerto de origen contendrá un número cualquiera que sirva para realizar esta distinción. Además, el programa cliente que realiza la petición también se debe conocer el número de puerto en el que se encuentra el servidor adecuado. Mientras que el programa del usuario utiliza números prácticamente aleatorios, el servidor deber tener asignado un número estándar para que pueda ser utilizado por el cliente. (Por ejemplo, en el caso de la transferencia de ficheros FTP el número oficial es el 21). Cuando es el servidor el que envía los datos, los números de puertos de origen y destino se intercambian.



En la transmisión de datos a través del protocolo TCP la fiabilidad es un factor muy importante. Para poder detectar los errores y pérdida de información en los datagramas, es necesario que el cliente envíe de nuevo al servidor unas señales de confirmación una vez que se ha recibido y comprobado la información satisfactoriamente. Estas señales se incluyen en el campo apropiado de la cabecera del datagrama (*Acknowledgment Number*), que tiene un tamaño de 32 bit. Si el servidor no obtiene la señal de confirmación adecuada transcurrido un período de tiempo razonable, el datagrama completo se volverá a enviar. Por razones de eficiencia los datagramas se envían continuamente sin esperar la confirmación, haciéndose necesaria la numeración de los mismos para que puedan ser ensamblados en el orden correcto.

2.1.7.2 IP (Internet Protocol)

El IP es un protocolo que pertenece al nivel de red, por lo tanto, es utilizado por los protocolos del nivel de transporte como TCP para encaminar los datos hacia su destino. IP tiene únicamente la misión de encaminar el datagrama, sin comprobar la integridad de la información que contiene. Para ello se utiliza una nueva cabecera que se antepone al datagrama que se está tratando. Suponiendo que el protocolo TCP ha sido el encargado de manejar el datagrama antes de pasarlo al IP, la estructura del mensaje una vez tratado quedaría así:

Cabecera (20 byte)	IP	Cabecera (20 byte)	TCP	Datos
-------------------------------	-----------	-------------------------------	------------	--------------

La cabecera IP tiene un tamaño de 160 bit y está formada por varios campos de distinto significado. Estos campos son:

- **Versión:** Número de versión del protocolo IP utilizado. Tendrá que tener el valor 4. *Tamaño: 4 bit.*



- **Longitud de la cabecera:** (*Internet Header Length, IHL*) Especifica la longitud de la cabecera expresada en el número de grupos de 32 bit que contiene. *Tamaño: 4 bit.*
- **Tipo de servicio:** El tipo o calidad de servicio se utiliza para indicar la prioridad o importancia de los datos que se envían, lo que condicionará la forma en que éstos serán tratados durante la transmisión. *Tamaño: 8 bit.*
- **Longitud total:** Es la longitud en bytes del datagrama completo, incluyendo la cabecera y los datos. Como este campo utiliza 16 bit, el tamaño máximo del datagrama no podrá superar los 65.535 bytes, aunque en la práctica este valor será mucho más pequeño. *Tamaño: 16 bit.*
- **Identificación:** Valor de identificación que se utiliza para facilitar el ensamblaje de los fragmentos del datagrama. *Tamaño: 16 bit.*
- **Flags:** Indicadores utilizados en la fragmentación. *Tamaño: 3 bit.*
- **Fragmentación:** Contiene un valor (*offset*) para poder ensamblar los datagramas que se hayan fragmentado. Está expresado en número de grupos de 8 bytes (64 bit), comenzando con el valor cero para el primer fragmento. *Tamaño: 16 bit.*
- **Límite de existencia:** Contiene un número que disminuye cada vez que el paquete pasa por un sistema. Si este número llega a cero, el paquete será descartado. Esto es necesario por razones de seguridad para evitar un bucle infinito, ya que aunque es bastante improbable que esto suceda en una red correctamente diseñada, no debe descuidarse esta posibilidad. *Tamaño: 8 bit.*
- **Protocolo:** El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. *Tamaño: 8 bit.*



- **Comprobación:** El campo de comprobación (*checksum*) es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del campo de comprobación de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el límite de existencia. *Tamaño: 16 bit.*
- **Dirección de origen:** Contiene la dirección del *host* que envía el paquete. *Tamaño: 32 bit.*
- **Dirección de destino:** Esta dirección es la del *host* que recibirá la información. Los *routers* o *gateways* intermedios deben conocerla para dirigir correctamente el paquete. *Tamaño: 32 bit.*

Organización de la cabecera IP.

Versión	IHL	Tipo de servicio	Longitud total	
Identificación			Flags	Fragmentación
Límite de existencia	Protocolo		Comprobación	
Dirección de origen				
Dirección de destino				



2.1.7.3 La dirección de Internet.

El protocolo IP identifica a cada ordenador que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bit que debe ser único para cada *host*, y normalmente suele representarse como cuatro cifras de 8 bit separadas por puntos.

La dirección de Internet (IP Address) se utiliza para identificar tanto al ordenador en concreto como la red a la que pertenece, de manera que sea posible distinguir a los ordenadores que se encuentran conectados a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron tres clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

- **Clase A:** Son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de los *hosts* que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de ordenadores en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que sólo puede haber 126 redes de este tamaño. ARPAnet es una de ellas, existiendo además algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una dirección de "clase A". Lo normal para las grandes organizaciones es que utilicen una o varias redes de "clase B".
- **Clase B:** Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del *host* permitiendo, por consiguiente, un número máximo de 64516 ordenadores en la misma red. Este tipo de direcciones tendría que ser



suficiente para la gran mayoría de las organizaciones grandes. En caso de que el número de ordenadores que se necesita conectar fuese mayor, sería posible obtener más de una dirección de "clase B", evitando de esta forma el uso de una de "clase A".

- **Clase C:** En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el *host*, lo que permite que se conecten un máximo de 254 ordenadores en cada red. Estas direcciones permiten un menor número de *host* que las anteriores, aunque son las más numerosas pudiendo existir un gran número redes de este tipo (más de dos millones).

Tabla de direcciones IP de Internet.

Clase	Primer byte	Identificación de red	Identificación de hosts	Número de redes	Número de hosts
A	1 .. 126	1 byte	3 byte	126	16.387.064
B	128 .. 191	2 byte	2 byte	16.256	64.516
C	192 .. 223	3 byte	1 byte	2.064.512	254

En la clasificación de direcciones anterior se puede notar que ciertos números no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como



es el caso de las direcciones cuyo primer byte sea superior a 223 (clases D y E, que aún no están definidas), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales. También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no pueden usarse normalmente por tener otros propósitos específicos.

El número 0 está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red para máquinas que aún no conocen el número de red a la que se encuentran conectadas, en la identificación de *host* para máquinas que aún no conocen su número de *host* dentro de la red, o en ambos casos.

El número 255 tiene también un significado especial, puesto que se reserva para el *broadcast*. El *broadcast* es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo datagrama a un número determinado de sistemas, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. Otra situación para el uso de *broadcast* es cuando se quiere convertir el nombre por dominio de un ordenador a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Lo usual es que cuando se quiere hacer uso del *broadcast* se utilice una dirección compuesta por el identificador normal de la red y por el número 255 (todo unos en binario) en cada byte que identifique al *host*. Sin embargo, por conveniencia también se permite el uso del número 255.255.255.255 con la misma finalidad, de forma que resulte más simple referirse a todos los sistemas de la red.

El *broadcast* es una característica que se encuentra implementada de formas diferentes dependiendo del medio utilizado, y por lo tanto, no siempre se encuentra disponible. En ARPAnet y en las líneas punto a punto no es posible enviar *broadcast*, pero sí que es posible hacerlo en las redes *Ethernet*, donde se supone que todos los ordenadores prestarán atención a este tipo de mensajes.



En el caso de algunas organizaciones extensas puede surgir la necesidad de dividir la red en otras redes más pequeñas (*subnets*). Como ejemplo podemos suponer una red de clase B que, naturalmente, tiene asignado como identificador de red un número de dos bytes. En este caso sería posible utilizar el tercer byte para indicar en qué red *Ethernet* se encuentra un *host* en concreto. Esta división no tendrá ningún significado para cualquier otro ordenador que esté conectado a una red perteneciente a otra organización, puesto que el tercer byte no será comprobado ni tratado de forma especial. Sin embargo, en el interior de esta red existirá una división y será necesario disponer de un software de red especialmente diseñado para ello. De esta forma queda oculta la organización interior de la red, siendo mucho más cómodo el acceso que si se tratara de varias direcciones de clase C independientes.

2.1.7.4 Servicios de Internet: el nivel de aplicación.

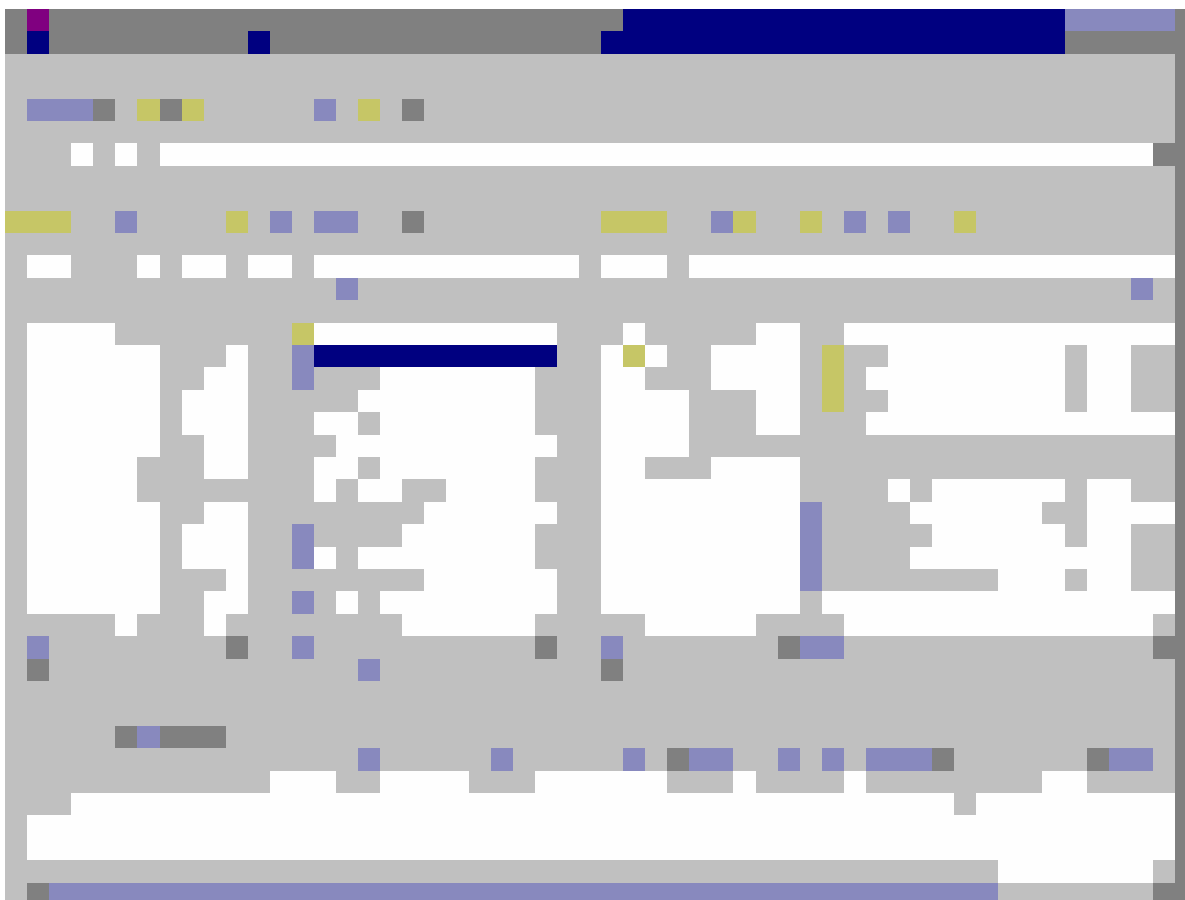
Los diferentes servicios a los que podemos tener acceso en Internet son proporcionados por los protocolos que pertenecen al nivel de aplicación. Estos protocolos forman parte del TCP/IP y deben aportar entre otras cosas una forma normalizada para interpretar la información, ya que todas las máquinas no utilizan los mismos juegos de caracteres ni los mismos estándares. Los protocolos de los otros niveles sólo se encargan de la transmisión de información como un bloque de bits, sin definir las normas que indiquen la manera en que tienen que interpretarse esos bits. Los protocolos del nivel de aplicación están destinados a tareas específicas, algunos de los cuales se consideran como tradicionales de Internet por utilizarse desde los inicios de la red, como son por ejemplo:

- Transferencia de ficheros (*File Transfer*).
- Correo electrónico (*e-mail*).
- Conexión remota (*remote login*).

**Transferencia de ficheros.**

El protocolo FTP (*File Transfer Protocol*) se incluye como parte del TCP/IP, siendo éste el protocolo de nivel de aplicación destinado a proporcionar el servicio de transferencia de ficheros en Internet. El FTP depende del protocolo TCP para las funciones de transporte, y guarda alguna relación con TELNET (protocolo para la conexión remota).

El protocolo FTP permite acceder a algún servidor que disponga de este servicio y realizar tareas como moverse a través de su estructura de directorios, ver y descargar ficheros al ordenador local, enviar ficheros al servidor o copiar archivos directamente de un servidor a otro de la red. Lógicamente y por motivos de seguridad se hace necesario contar con el permiso previo para poder realizar todas estas operaciones. El servidor FTP pedirá el nombre de usuario y clave de acceso al iniciar la sesión (*login*), que debe ser suministrado correctamente para utilizar el servicio.



La manera de utilizar FTP es por medio de una serie de comandos, los cuales suelen variar dependiendo del sistema en que se esté ejecutando el programa, pero básicamente con la misma funcionalidad. Existen aplicaciones de FTP para prácticamente todos los sistemas operativos más utilizados, aunque hay que tener en cuenta que los protocolos TCP/IP están generalmente muy relacionados con sistemas UNIX. Por este motivo y, ya que la forma en que son listados los ficheros de cada directorio depende del sistema operativo del servidor, es muy frecuente que esta información se muestre con el formato propio del UNIX. También hay que mencionar que en algunos sistemas se han desarrollado clientes de FTP que cuentan con un interfaz gráfico de usuario, lo que facilita notablemente su utilización, aunque en algunos casos se pierde algo de funcionalidad.



Existe una forma muy utilizada para acceder a fuentes de archivos de carácter público por medio de FTP. Es el acceso FTP anónimo, mediante el cual se pueden copiar ficheros de los *hosts* que lo permitan, actuando estos *host* como enormes almacenes de información y de todo tipo de ficheros para uso público. Generalmente el acceso anónimo tendrá algunas limitaciones en los permisos, siendo normal en estos casos que no se permita realizar acciones tales como añadir ficheros o modificar los existentes. Para tener acceso anónimo a un servidor de FTP hay que identificarse con la palabra "anonymous" como el nombre de usuario, tras lo cual se pedirá el *password* o clave correspondiente. Normalmente se aceptará cualquier cadena de caracteres como clave de usuario, pero lo usual es que aquí se indique la dirección de correo electrónico propia, o bien la palabra "guest". Utilizar la dirección de correo electrónico como clave de acceso es una regla de cortesía que permite a los operadores y administradores hacerse una idea de los usuarios que están interesados en el servicio, aunque en algunos lugares puede que se solicite esta información rechazando el uso de la palabra "guest".

El FTP proporciona dos modos de transferencia de ficheros: ASCII y binario. El modo de transferencia ASCII se utiliza cuando se quiere transmitir archivos de texto, ya que cada sistema puede utilizar un formato distinto para la representación de texto. En este caso se realiza una conversión en el formato del fichero original, de manera que el fichero recibido pueda utilizarse normalmente. El modo de transferencia binario se debe utilizar en cualquier otro caso, es decir, cuando el fichero que vamos a recibir contiene datos que no son texto. Aquí no se debe realizar ninguna conversión porque quedarían inservibles los datos del fichero.

Conexión remota.

El protocolo diseñado para proporcionar el servicio de conexión remota (*remote login*) recibe el nombre de TELNET, el cual forma parte del conjunto de protocolos TCP/IP y depende del protocolo TCP para el nivel de transporte.



El protocolo TELNET es un emulador de terminal que permite acceder a los recursos y ejecutar los programas de un ordenador remoto en la red, de la misma forma que si se tratara de un terminal real directamente conectado al sistema remoto. Una vez establecida la conexión el usuario podrá iniciar la sesión con su clave de acceso. De la misma manera que ocurre con el protocolo FTP, existen servidores que permiten un acceso libre cuando se especifica "anonymous" como nombre de usuario.

Es posible ejecutar una aplicación cliente TELNET desde cualquier sistema operativo, pero hay que tener en cuenta que los servidores suelen ser sistemas VMS o UNIX por lo que, a diferencia del protocolo FTP para transferencia de ficheros donde se utilizan ciertos



comandos propios de esta aplicación, los comandos y sintaxis que se utilice en TELNET deben ser los del sistema operativo del servidor. El sistema local que utiliza el usuario se convierte en un terminal "no inteligente" donde todos los caracteres pulsados y las acciones que se realicen se envían al *host* remoto, el cual devuelve el resultado de su trabajo. Para facilitar un poco la tarea a los usuarios, en algunos casos se encuentran desarrollados menús con las distintas opciones que se ofrecen.

Los programas clientes de TELNET deben ser capaces de emular los terminales en modo texto más utilizados para asegurarse la compatibilidad con otros sistemas, lo que incluye una emulación del teclado. El terminal más extendido es el VT100, el



cual proporciona compatibilidad con la mayoría de los sistemas, aunque puede ser aconsejable que el programa cliente soporte emulación de otro tipo de terminales.

Correo electrónico.

El servicio de correo electrónico se proporciona a través del protocolo SMTP (*Simple Mail Transfer Protocol*), y permite enviar mensajes a otros usuarios de la red. A través de estos mensajes no sólo se puede intercambiar texto, sino también archivos binarios de cualquier tipo.

Generalmente los mensajes de correo electrónico no se envían directamente a los ordenadores personales de cada usuario, puesto que en estos casos puede ocurrir



que esté apagado o que no esté ejecutando la aplicación de correo electrónico. Para evitar este problema se utiliza un ordenador más grande como almacén de los mensajes recibidos, el cual actúa como servidor de correo electrónico permanentemente. Los mensajes permanecerán en este sistema hasta que el usuario los transfiera a su propio ordenador para leerlos de

forma local.

2.1.8 Modelo jerárquico ISO/OSI

En la industria se aceptó hace ya bastante tiempo, la necesidad de estándares que gobernarán las acciones y las características físicas y eléctricas de los equipos de comunicación. Este punto de vista, sin embargo ha tardado en imponerse en la industria de los ordenadores.



Entre las organizaciones más importantes que han colaborado en el desarrollo de estándares en nuestra área tenemos:

ISO (*International Organization for Standardization*): Agrupa a 89 países, se trata de una organización voluntaria, no gubernamental, cuyos miembros han desarrollado estándares para las naciones participantes. Uno de sus comités se ocupa de los sistemas de información. Han desarrollado el modelo de referencia **OSI** (Open Systems Interconnection) y protocolos estándar para varios niveles del modelo.

CCITT (*Comité Consultatif International de Télégraphique et Téléphonique*): Organización de la Naciones Unidas constituida, en principio, por las autoridades de Correos, Telégrafos y Teléfonos (PTT) de los países miembros. Estados Unidos está representado por el departamento de Estado. Se encarga de realizar recomendaciones técnicas sobre teléfono, telégrafo e interfaces de comunicación de datos, que a menudo se reconocen como estándares. Trabaja en colaboración con **ISO** (que en la actualidad es miembro de CCITT).

EIA (*Electronic Industries Association*): Asociación vinculada al ámbito de la electrónica. Es miembro de **ANSI**. Sus estándares se encuadran dentro del nivel 1 del modelo de referencia **OSI**.

ANSI (*American National Standard Institute*): Asociación con fines no lucrativos, formada por fabricantes, usuarios, compañías que ofrecen servicios públicos de comunicaciones y otras organizaciones interesadas en temas de comunicación. Es el representante estadounidense en **ISO**. Que adopta con frecuencia los estándares **ANSI** como estándares internacionales.



La aceptación mayoritaria de los diferentes estándares ha supuesto un crecimiento de la oferta de equipos compatibles de diversos fabricantes, proporcionando a los usuarios una mayor libertad de elección, favoreciendo la competencia entre fabricantes e incrementando la demanda de equipos compatibles.

Sin embargo los estándares llevan también aparejados ciertos inconvenientes, como puede ser la introducción de retraso tecnológico, que ralentiza nuevos desarrollos y la multiplicidad de estándares no compatibles.

En 1977 la Organización Internacional De Estandarización ISO estableció un subcomité encargado de diseñar una arquitectura de comunicación. El resultado fue el *Modelo de referencia para la Interconexión de Sistemas Abiertos OSI*, adoptado en 1983, que establece unas bases que permiten conectar sistemas *abiertos* para procesamiento de aplicaciones distribuidas. Se trata de un marco de referencia para definir estándares que permitan comunicar ordenadores heterogéneos.

Dicho modelo define una arquitectura de comunicación estructurada en siete niveles verticales. Cada nivel ejecuta un subconjunto de las funciones que se requieren para comunicar con el otro sistema. Para ello se apoya en los servicios que le ofrece el nivel inmediato inferior y ofrece sus servicios al nivel que está por encima de él. Idealmente, los cambios que se realicen en un nivel no deberían afectar a su nivel vecino mientras ni se modifiquen los servicios que le ofrece.

La tarea del subcomité ISO fue definir el conjunto de niveles y los servicios proporcionados por cada nivel. Los principios aplicados para establecer un nivel fueron los siguientes:

Diferentes niveles deben corresponder a diferentes niveles de abstracción en el manejo de los datos (por ejemplo diferencias en la morfología, la sintaxis, la semántica).

Cada nivel debe ejecutar una función bien definida.



Aprovechar la experiencia de protocolos anteriores. Las fronteras de niveles deben situarse donde la experiencia ha demostrado que son convenientes.

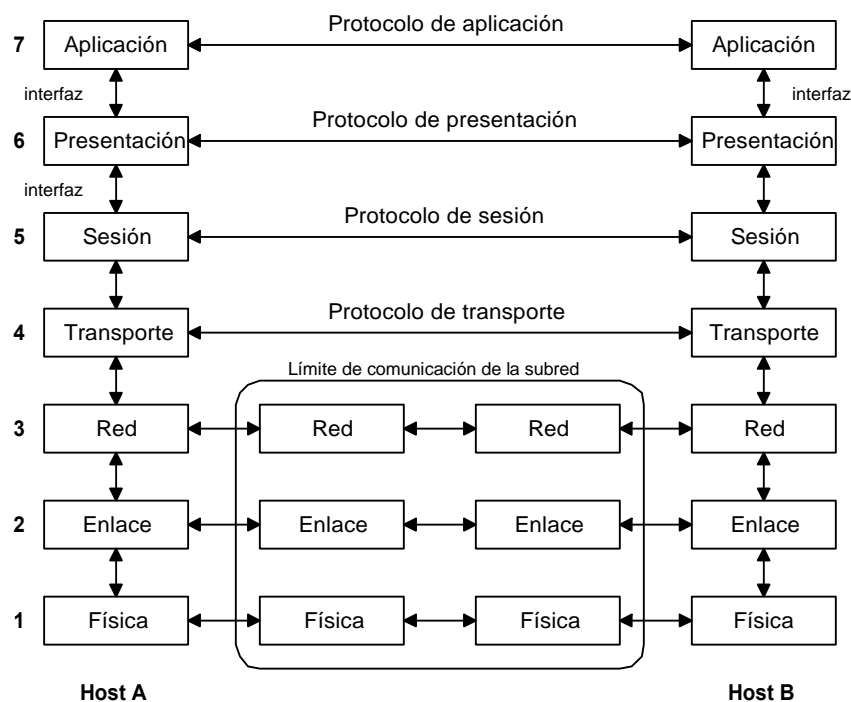
Establecer las divisiones de los niveles de forma que se minimice el flujo de información entre ellos.

El número de niveles debe ser suficiente para que no agrupen funciones distintas, pero no tan grande que haga la arquitectura inmanejable.

Permitir que las modificaciones de funciones o protocolos que se realicen en un nivel no afecten a los niveles contiguos.

Cada nivel debe interaccionar únicamente con los niveles contiguos a él (superior e inferiormente).

2.1.8.1 Niveles OSI



Arquitectura de red en el modelo OSI



Los siete niveles que configuran el modelo OSI suelen agruparse en dos bloques. Los tres niveles inferiores (nivel físico, nivel de enlace y nivel de red) constituyen el bloque de transmisión. Son niveles dependientes de la red de conmutación utilizada para la comunicación entre los dos sistemas. Por el contrario, los tres niveles superiores (nivel de sesión, de presentación y de aplicación) son niveles orientados a la aplicación y realizan funciones directamente vinculadas con los procesos de aplicación que desean comunicarse. El nivel intermedio (nivel de transporte) enmascara a los niveles orientados a la aplicación, el funcionamiento detallado de los niveles dependientes de la red.

Pasemos a discutir brevemente cada nivel:

Nivel físico: El nivel físico se ocupa de la transmisión de bits a través de un canal de comunicación. Regula aspectos de la comunicación como el tipo de señal, el esquema de codificación, el modo de comunicación (dúplex, semi-dúplex o símplex) y, en general, todas las cuestiones eléctricas, mecánicas y de procedimiento en la interfaz física entre los dispositivos que se comunican.

Nivel de enlace de datos: Mientras el nivel físico proporciona únicamente un servicio de transmisión de bits a través de una canal, el nivel de enlace tiene el objetivo de hacer la comunicación fiable y proporcionar los medios para activar, mantener y desconectar el enlace. El principal servicio proporcionado por este nivel es el de detección y control de errores. Con un protocolo suficientemente elaborado, el nivel de red puede asumir una transmisión libre de errores a través del enlace. Pero, hay que tener en cuenta, que si los sistemas que se comunican no están directamente conectados, sino a través de varios enlaces, cada uno funcionará de forma independiente y los niveles superiores no estarán eximidos de la responsabilidad de controlar los errores.



Nivel de Red: El servicio básico de este nivel es proporcionar transferencia de datos transparente entre entidades de transporte. Es decir, libera al nivel de transporte de la necesidad de conocer el funcionamiento interno de la subred. Entre sus principales funciones se encuentran el encaminamiento y el control de la congestión.

Nivel de Transporte: Es el primer nivel que lleva a cabo comunicación *extremo - extremo*, condición que se mantiene en los niveles superiores a él. Su objetivo es proporcionar mecanismos que garanticen que el intercambio de datos entre procesos de distintos sistemas se lleve a cabo de forma fiable. El nivel de transporte debe asegurar que los paquetes de datos se entregan libres de error, ordenadas y sin pérdidas ni duplicados. Puede también optimizar el uso de los servicios de red (por ejemplo mediante multiplexación) y proporcionar la calidad de servicio solicitada por los servicios de sesión.

El tamaño y la complejidad de un protocolo de transporte dependen del tipo de servicio proporcionado por el nivel de red. Con un servicio de red fiable, orientado a la conexión, un protocolo de transporte mínimo resultará suficiente. Por el contrario, si el nivel 3 proporciona un servicio no fiable y/o basado en datagramas el protocolo de transporte debe incluir detección y recuperación de errores. De acuerdo con esto, **ISO** ha definido cinco clases de protocolo de transporte orientados a distintos tipos de servicios de red. Otro estándar de protocolo de transporte ampliamente extendido – aunque fuera del entorno **ISO** – es el protocolo **TCP**.

Nivel de sesión: Este nivel proporciona los mecanismos para controlar el diálogo entre aplicaciones. Como mínimo el nivel de sesión proporciona un medio para que dos procesos de aplicación puedan establecer y utilizar una conexión, llamada **sesión**. Además de esto, puede proporcionar una serie de servicios de mejora sobre el nivel de transporte, como son:

- 1 Gestión del diálogo, mediante la utilización de testigos.



2 Mecanismos de recuperación (*checkpointing*).

Nivel de Presentación: A diferencia de los niveles anteriores, interesados en la fiabilidad de los datos que se transmiten, el nivel de presentación se ocupa de aspectos sintácticos y semánticos de la información transmitida.

Un ejemplo típico de un servicio de presentación es la codificación de datos de una forma estándar. Cada ordenador tiene su propia forma de representar strings de caracteres (ASCII, EBCDIC, etc), enteros (complemento a uno, dos, etc) números en coma flotante y estructuras compuestas. Para hacer posible la comunicación entre computadoras con distintos esquemas de representación. Las estructuras de datos pueden definirse durante la comunicación. El trabajo de gestionar estas estructuras de datos y convertirlas de la representación usada en el ordenador a la representación estándar y viceversa, es realizado por el nivel de presentación. Además de lo anterior, este nivel maneja otros aspectos de representación de la información como compresión de datos y cifrado.

Nivel de aplicación: El nivel de aplicación proporciona un medio a los procesos de aplicación para acceder al entorno OSI. Contiene funciones de gestión y mecanismos útiles para soportar aplicaciones distribuidas. Ejemplos de protocolos a este nivel son los de transferencia de ficheros y correo electrónico.

2.1.8.2 Servicios

Las entidades en un nivel N ofrecen servicios que son utilizados por las entidades del nivel $N+1$. El nivel N es, entonces, el proveedor del servicio y el nivel $N+1$ el usuario del servicio. A su vez, el nivel N para proporcionar sus servicios puede utilizar los servicios que le ofrece el nivel $N-1$.

Los servicios se hacen disponibles en los SAP (Puntos de acceso al servicio). Los SAPs del Nivel N son los puntos donde el nivel $N+1$ puede acceder a los servicios ofrecidos.



Un servicio es invocado por el usuario, o es indicado por el proveedor del servicio mediante el intercambio de un conjunto de primitivas de servicio a través de la interfaz entre los niveles implicados. En el modelo OSI, estas primitivas se dividen en cuatro clases:

Request: Una entidad solicita el servicio.

Indication: Una entidad es informada de algún evento.

Response: Una entidad quiere responder a un evento.

Confirm: Una entidad es informada sobre su solicitud.

Los servicios pueden ser confirmados o no confirmados. Un servicio confirmado utiliza las cuatro primitivas request, indication, response y confirm. Un servicio no confirmado sólo requiere primitivas request e indication. El establecimiento de la conexión siempre es un servicio confirmado, mientras que la transferencia de datos puede ser confirmada o no, dependiendo de que el emisor necesite o no un reconocimiento.

Los niveles pueden ofrecer dos tipos básicos de servicio: sin conexión y orientados a conexión. La *conexión* permitirá establecer unos parámetros generales para toda la comunicación, agrupando los diferentes mensajes en un marco común.

En los servicios sin conexión la información recibida por cada nivel es procesada de forma autónoma, independientemente de la que haya recibido anteriormente. Es un servicio similar al ofrecido por correos, en el cual cada carta viaja de forma independiente de las anteriores.

Se pueden distinguir dos modelos de servicios sin conexión:

Datagrama: Consiste en enviar la información y despreocuparse de ella. Por



ello se le suele denominar *Send & Pray (Sueña y Reza)*. Este servicio sería equivalente al correo ordinario, en el cual enviamos una carta y no obtenemos confirmación de su llegada.

Con acuse de recibo (Asentimiento): El receptor tiene que enviar un reconocimiento de que ha recibido la información.

Los servicios orientados a conexión corresponden al modelo del sistema telefónico. Cada mensaje enviado es interpretado en un contexto formado por los mensajes anteriores y posteriores, de forma que forman una unidad. Para ellos es necesario que se cumplan tres fases:

Establecimiento de la conexión.

Utilización.

Desconexión, o cierre de la conexión.

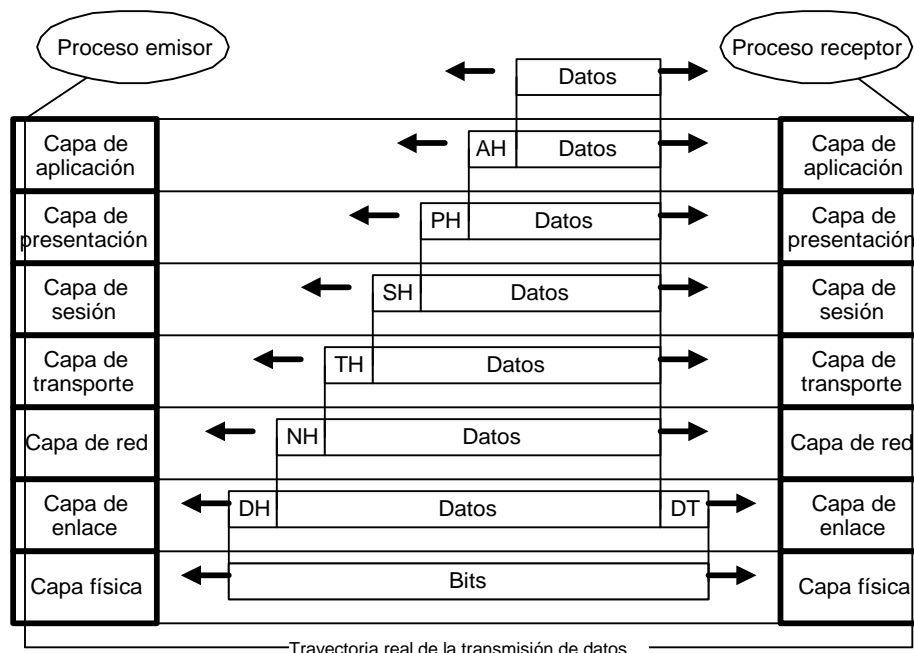
2.1.8.3 Transmisión de datos en el modelo OSI

En el esquema OSI se pretende implementar la comunicación de aplicaciones de usuario mediante la utilización de servicios proporcionados por los niveles inferiores. Ambas aplicaciones tendrán una unidad de información básica a intercambiar, cumpliendo su protocolo establecido de nivel de aplicación. Debemos conseguir que esta información transmitida llegue tal y como fue enviada al nivel de aplicación del host receptor.

Sin embargo, y para asegurar el cumplimiento de sus funciones, en cada nivel es necesario utilizar cierta información de control que sólo será interpretada por el nivel equivalente de la máquina receptora. Por ejemplo, para que el nivel de red de los distintos IMPs por los que pasará la información puedan enviar correctamente la misma, es necesario conocer las direcciones en la red de las máquinas origen y destino de los datos, pero esta información no tiene por qué ser conocida por el nivel



de transporte ni por el de enlace de datos. De hecho, y para proteger la independencia de niveles, resulta aconsejable que cada información de control sea exclusiva del nivel que la requiera. Cada nivel, pues, tratará la información procedente del nivel superior como si fueran datos en su integridad, y añadirá su propia información de control (cabecera) antes de pasarlo al nivel inferior.



Transmisión de datos en el modelo OSI

Como puede verse, cada nivel añade información a transmitir para cumplir su protocolo, tratando la información de control añadida por el nivel anterior como datos. Los términos AH, PH, etc, denotan las cabeceras añadidas por cada uno de los niveles (Application Header, Presentation Header, etc).

A pesar de que la comunicación se realiza verticalmente (entre niveles) hay que tener en cuenta la existencia de los protocolos a cada nivel.



2.2 Virus informáticos.

Hay numerosos estudios eruditos que intentan determinar la paternidad de la idea de los virus Informáticos. Es muy difícil saber con exactitud quién habló por vez primera sobre algo parecido a un código con las características de un virus.

Quizás el primero que adelantó una definición de lo que entonces no existía todavía fue el matemático **John von Neumann** (a la derecha) al publicar en 1949 un artículo titulado “Theory and Organization of Complicated Automata” hablando de “una porción de código capaz de reproducirse a sí mismo”.



Se inician las “Core Wars” (guerras del núcleo) a finales de los 50, desarrolladas por H. Douglas McIlroy, Victor Vysotsky y Robert Morris Sr. (sí, el padre del otro, el del Gusano), investigadores de inteligencia artificial de los laboratorios Bell. Dos programas hostiles, escritos en un lenguaje pseudo-ensamblador llamado RedCode, podían crecer en memoria y luchar entre sí. Consiguieron su “guerrero” más perfecto al que llamaron “Gemini”. La película “Tron” de 1982 no es ajena a esto.

En 1970 Bob Thomas creó un programa al que llamó “Creeper” (reptador) que viajaba por las redes y era usado por los controladores aéreos para ceder el control de un avión de una terminal a otro.

A principios de los 80, John Shock y Jon Hupp, del centro de investigación Xerox de Palo Alto, California, diseñaron un programa-gusano para intercambio de mensajes y tareas automáticas durante la noche, pero se puso a trabajar de forma incontrolada y tuvieron que eliminarlo.



En 1983 Ken Thompson recibía el premio Alan Turing y sorprendía a todo el mundo



con un discurso basado en las “Core Wars”, en el que estimulaba a todos los usuarios y programadores a experimentar con esas “criaturas lógicas”. Por cierto, este “vándalo” fue el **creador de UNIX en 1969**.

En 1984 y en años sucesivos, apareció en la prestigiosa revista norteamericana “Scientific American” una serie de artículos de A. K. Dewney en los que revelaba al gran público la existencia y las características de las “Core Wars”.

En 1985 un estudiante de la Universidad de California del Sur llamado Fred Cohen (foto dcha.) completaba su tesis sobre programas autoduplicadores (iniciada en 1983). Fue en realidad el director de su tesis el que le sugirió el nombre de “virus informático”. Había publicado un artículo en “IFIPsec 84” titulado “Computer Viruses. Theory and experiments”, en el que establecía una definición académica del virus informático como: “un programa que puede infectar a otros programas incluyendo una copia posiblemente evolucionada de sí mismo”.

Se puede decir que es en el año 1986 cuando aparecen los primeros virus en el sentido que le damos hoy al término. Los virus para Apple II, especialmente Elk Cloner, y los ensayos académicos de Cohen tienen otra consideración.

En enero de 1986 aparece en escena el virus “Brain”, procedente de Paquistán. Fue el primer virus para PC, capaz de infectar el sector de arranque y de ocultarse (técnica stealth). En ese mismo año, Ralf Burger creó el virus “Virdem”, el primero que podía infectar ficheros ejecutables, en este caso sólo los COM (más simples y sencillos de infectar). Lo distribuyó en la reunión del Chaos Computer Club en Alemania en diciembre de ese año. Estaban definidos los dos tipos básicos de virus según el soporte infectado, aunque la constante es que se pretendía infectar código



ejecutable estuviera en el sector de arranque de un disquete o en un programa ejecutable. A la espera de un tercer tipo: los interpretados (macro y scripts), en los que el código vírico actúa cuando se “ejecuta” el archivo de texto en el que va escondido.

En 1987 tenemos al virus "Stoned" (origen de uno de los más famosos de todos los tiempos: el "Michelangelo"). La película “Hackers”, odiada y amada a partes iguales, hace referencia a cierto gusano parecido al de Morris y a un virus en el que no es difícil ver un recuerdo de Michelangelo (lo llaman Leonardo da Vinci). También se tiene noticia del "Lehigh" (relacionado con pruebas de Cohen y Ken van Wyk, al parecer) y del famosísimo "Vienna" (cuya inclusión del código desamblado en un libro por Ralf Burger provocó un gran escándalo).

Y llegó 1988, año de la mayoría de edad de los virus y gusanos. Nadie volvería a decir que eran producto de la imaginación, leyendas urbanas, “leyendas comparables a la de los gnomos”. No voy a traer a estas páginas (o pantallas) ejemplos de aquellos años para no sonrojar a decenas de expertos que se cubrieron de gloria acerca de la inexistencia e imposibilidad de los virus informáticos ;) Bueno, sí lo haré en el futuro libro.

El viernes 13 de mayo de 1988 el virus “Jerusalem” o “Friday the 13th”, conocido como "Viernes 13" comenzó a propagar el miedo entre los usuarios de todo el mundo. Este es el primer pánico asociado a un virus.

El 2 de noviembre de ese año fue liberado el gusano de Morris o “gusano de Internet” que colapsó un 10% de ARPANET. Creado por un estudiante norteamericano llamado Robert Tappan Morris. El caos generado por el pánico superó a los efectos técnicos reales.



En 1989 se inicia lo que se conocerá más tarde como la “factoría búlgara”, dada la cantidad y calidad de virus creados en ese país. Destacan los virus "Eddie", "Nomenklatura" (que afectó al gobierno británico con especial intensidad), "Dark Avenger", "el Número de la Bestia", etc. El libro “Los piratas del chip” de Clouhg y Mungo (Approaching Zero) relata de forma muy amena e interesante estos sucesos, especialmente la “evolución” del virus "Yankee Doodle" y la extraña relación del creador de virus “Dark Avenger” con el periodista de asuntos informáticos Vesselin Bontchev.

Los primeros años 90 vieron la aparición del polimorfismo, de los primeros grupos de escritores y de los ezines, forma principal de comunicación entre los investigadores de la vida artificial, junto a los foros que se formaban en torno a BBS (ordenadores que mantenían un programa para recibir conexiones de otros ordenadores a través de la línea telefónica).

Con la aparición del **Windows 95** se revoluciona el mundo vírico. Tras un período de desconcierto, se producen las primeras creaciones para el nuevo sistema operativo...



Fueron "Boza" (de forma imperfecta) y "Win32.Jacky", de Jacky Querty (ya perfeccionada) los que encontraron el camino de la infección y abrieron la vía para los demás. En este año se realiza el primer virus de macro para Word: "Concept" (ya existían en Mac).



A finales de los 90, la creciente generalización de Internet hace que los virus y gusanos aprovechen este medio para propagarse velozmente por todo el mundo (correo, lenguajes de script, etc).

En 1998, el virus "CIH", más conocido como "Chernobyl", produce **daños en la BIOS** y obliga a quitar la placa base en determinados PCs. La noticia de “un virus que daña el hardware” inunda los medios.

En 1999, David L. Smith revoluciona ciertos aspectos de la seguridad con su gusano de macro "Melissa". Fue un auténtico fenómeno periodístico (mediático que dirían hoy) a nivel mundial. Ninguno se había extendido con tal velocidad hasta entonces. Aprovecha la libreta de direcciones del ordenador infectado para propagarse.

El año 2000 es el año del gusano "ILOVEYOU". El uso de la ingeniería social puso en evidencia el eslabón más débil de la seguridad en muchos sitios: el factor humano.



La explosión de los gusanos de Internet (I-Worm) tuvo lugar en el 2001. "SirCam" (gusano mexicano), "CodeRed" (aprovecha un fallo o bug del IIS), "Nimda" (inspirado en los anteriores), "BadTrans", etc.

El prestigioso coder brasileño Vecna liberó "Hybris", auténtica delicia para los estudiosos y pesadilla para los demás mortales. Los años 2002 y 2003 han generado noticias especialmente impactantes, pero el número de virus, gusanos y demás malware se ha disparado hasta niveles... ¿preocupantes? , por lo que los medios de comunicación no pueden darle el relieve que tuvieron aquellos míticos de 1988, 1999 o 2000.



2.2.1 Qué son los virus informáticos.

Es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este. Decimos que es un programa parásito porque el programa ataca a los archivos o sector es de "booteo" y se replica a sí mismo para continuar su esparcimiento.

Algunos se limitan solamente a replicarse, mientras que otros pueden producir serios daños que pueden afectar a los sistemas. Se ha llegado a un punto tal, que un nuevo



virus llamado W95/CIH-10xx. o también como CIH.Spacefiller (puede aparecer el 26 de cada mes, especialmente 26 de Junio y 26 de Abril) ataca al BIOS de la PC huésped y cambiar su configuración de tal forma que se requiere cambiarlo. Nunca se puede asumir que un virus es inofensivo y dejarlo "flotando" en el sistema.

Existen ciertas analogías entre los virus biológicos y los informáticos: mientras los primeros son agentes externos que invaden células para alterar su información genética y reproducirse, los segundos son programas-rutinas, en un sentido más estricto, capaces de infectar archivos de computadoras, reproduciéndose una y otra vez cuando se accede a dichos archivos, dañando la información existente en la memoria o alguno de los dispositivos de almacenamiento del ordenador.

Tienen diferentes finalidades: Algunos sólo 'infectan', otros alteran datos, otros los eliminan, algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: **PROPAGARSE.**

Es importante destacar que ***el potencial de daño de un virus informático no depende de su complejidad sino del entorno donde actúa.***



La definición más simple y completa que hay de los virus corresponde al modelo D. A. S., y se fundamenta en tres características, que se refuerzan y dependen mutuamente. Según ella, un virus es un programa que cumple las siguientes pautas:

- ❑ Es dañino
- ❑ Es auto reproductor
- ❑ Es subrepticio

Al igual que en el reino animal, establecer una taxonomía o clasificación de las especies y subespecies de virus y códigos “*malignos*” en general es extremadamente difícil, especialmente teniendo en cuenta que muchas “*criaturas*” comparten características de varias especies. Virus, gusanos, troyanos, bombas lógicas, “*malware*” en general, forman una fauna de gran riqueza y variedad.

Se impone establecer una definición básica y sencilla de cada tipo:

2.2.2 Clasificación de virus informáticos.

VIRUS. Programa con capacidad reproductiva (replicación) que infecta ficheros como medio de propagación (y estos ejecutables infectados “viajan” a través de disquetes, cdroms o descargas por Internet). Ejemplos: Brain, Virdem, Stoned, Viernes 13, Michelangelo, Win32.Jacky, CIH-Chernobil, etc.

Los virus se clasifican por el modo en que actúan infectando la computadora:

- **Programa:** Infectan archivos ejecutables tales como .com / .exe / .ovl / .drv / .sys / .bin
- **Boot:** Infectan los sectores Boot Record, Master Boot, FAT y la Tabla de Partición.
- **Múltiples:** Infectan programas y sectores de “booteo”.
- **Bios:** Atacan al Bios para desde allí reescribir los discos duros.



- **Hoax:** Se distribuyen por e-mail y la única forma de eliminarlos es el uso del sentido común.

GUSANO. Programa que genera copias de sí mismo (igual que un virus) pero no se “pega” a ningún fichero ejecutable y se envía a través de una red. Ejemplos: Gusano de Morris, Melissa, Iloveyou, CodeRed, SirCam, Nimda, Slammer.

TROYANO. Programa o código oculto dentro de otro programa de interés para el usuario con el objeto de que el usuario confíe en su ejecución, a semejanza del episodio del regalo del caballo de Troya (carácter estático). Ejemplos: Back Orifice o BO, SubSeven, Netbus, Assasin, Optix, Ptakss, Cabronator, etc.

BOMBA LÓGICA. Instrucciones malignas camufladas en el código de un programa que se activan según determine el programador (en una fecha, por medio de una tecla o al no cumplirse una exigencia). Ejemplo: el caso más típico es el programador que al no recibir el pago por su trabajo activa o no inutiliza la orden que ejecuta el código cuya misión puede ser borrar, encriptar, etc.

2.2.3 Cómo funcionan los virus informáticos.

El hecho de que la definición imponga que los virus son programas no admite ningún tipo de observación; está extremadamente claro que son programas, realizados por personas. Además de ser programas tienen el fin ineludible de causar daño en cualquiera de sus formas.

Asimismo, se pueden distinguir tres módulos principales de un virus informático:

- Módulo de Reproducción
- Módulo de Ataque



➤ Módulo de Defensa

El **módulo de reproducción** se encarga de manejar las rutinas de "parasitación" de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse subrepticamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.

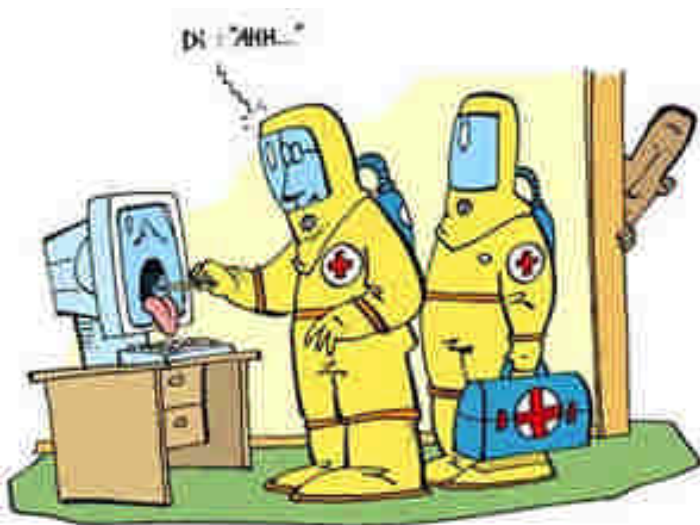
El **módulo de ataque** es optativo. En caso de estar presente es el encargado de manejar las rutinas de daño adicional del virus. Por ejemplo, el conocido virus **Michelangelo**, se aloja en el boot sector, y en los discos rígidos en la tabla de particiones, y tiene un módulo de ataque que se activa cuando el reloj de la computadora indica 6 de Marzo. En estas condiciones la rutina actúa sobre la información del disco rígido volviéndola inutilizable.

El módulo de defensa tiene, obviamente, la misión de proteger al virus y, como el de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la remoción del virus y retardar, en todo lo posible, su detección.

2.2.4 Cómo se eliminan los virus informáticos.

No para toda enfermedad existe cura, como tampoco existe una forma de erradicar todos y cada uno de los virus existentes.

Es importante aclarar que todo antivirus es un programa y que, como todo programa, sólo funcionará





correctamente si es adecuado y está bien configurado. Además, un antivirus es una herramienta para el usuario y no sólo **no será eficaz para el 100% de los casos**, sino que **nunca será una protección total ni definitiva**.

La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independientemente de las prestaciones adicionales que pueda ofrecer, puesto que el hecho de detectar la posible presencia de un virus informático, detener el trabajo y tomar las medidas necesarias, es suficiente para acotar un buen porcentaje de los daños posibles. Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una entidad infectada.

El modelo más primario de las funciones de un programa antivirus es la detección de su presencia y, en lo posible, su identificación. La primera técnica que se popularizó para la detección de virus informáticos, y que todavía se sigue utilizando (aunque cada vez con menos eficiencia), es la técnica de **scanning**. Esta técnica consiste en revisar el código de todos los archivos contenidos en la unidad de almacenamiento - fundamentalmente los archivos ejecutables- en busca de pequeñas porciones de código que puedan pertenecer a un virus informático. Este procedimiento, denominado **escaneo**, se realiza a partir de una base de datos que contiene trozos de código representativos de cada virus conocido, agregando el empleo de determinados algoritmos que agilizan los procesos de búsqueda.

La técnica de **scanning** fue bastante eficaz en los primeros tiempos de los virus informáticos, cuando había pocos y su producción era pequeña. Este relativamente pequeño volumen de virus informáticos permitía que los desarrolladores de antivirus escaneadores tuvieran tiempo de analizar el virus, extraer el pequeño trozo de código que lo iba a identificar y agregarlo a la base de datos del programa para lanzar una nueva versión. Sin embargo, la obsolescencia de este mecanismo de



identificación como una solución antivirus completa se encontró en su mismo modelo.

El primer punto grave de este sistema radica en que siempre brinda una solución *a posteriori*: es necesario que un virus informático alcance un grado de dispersión considerable para que sea enviado (por usuarios capacitados, especialistas o distribuidores del producto) a los desarrolladores de antivirus. Estos lo analizarán, extraerán el trozo de código que lo identificará, y lo incluirán en la próxima versión de su programa antivirus. Este proceso puede demorar meses a partir del momento en que el virus comienza a tener una dispersión considerable, lapso en el cual puede causar graves daños sin que pueda ser identificado.

Además, este modelo consiste en una sucesión infinita de soluciones parciales y momentáneas (cuya sumatoria jamás constituirá una solución definitiva), que deben actualizarse periódicamente debido a la aparición de nuevos virus.

En síntesis, la técnica de scanning es altamente ineficiente, pero se sigue utilizando debido a que permite identificar rápidamente la presencia de los virus más conocidos y, como son estos los de mayor dispersión, permite una importante gama de posibilidades. Un ejemplo típico de un antivirus de esta clase es el Viruscan de McAfee.





En virtud del pronto agotamiento técnico de la técnica de scanning, los desarrolladores de programas antivirus han dotado a sus creaciones de métodos para búsquedas de virus informáticos (y de sus actividades), que no identifican específicamente al virus sino a algunas de sus características generales y comportamientos universalizados.

Este tipo de método rastrea rutinas de alteración de información que no puedan ser controladas por el usuario, modificación de sectores críticos de las unidades de almacenamiento (master boot record, boot sector, FAT, entre otras), etc.

Un ejemplo de este tipo de métodos es el que utiliza algoritmos **heurísticos**.

De hecho, esta naturaleza de procedimientos busca, de manera bastante eficiente, códigos de instrucciones potencialmente pertenecientes a un virus informático. Resulta eficaz para la detección de virus conocidos y es una de las soluciones utilizadas por los antivirus para la detección de nuevos virus. El inconveniente que presenta este tipo de algoritmo radica en que puede llegar a sospecharse de muchas cosas que no son virus. Esto hace necesario que el usuario que lo utiliza conozca un poco acerca de la estructura del sistema operativo, a fin de poseer herramientas que le faciliten una discriminación de cualquier falsa alarma generada por un método heurístico. Algunos de los antivirus de esta clase son F-Prot, Norton AntiVirus y Dr. Solomon's Toolkit.





Ahora bien, otra forma de detectar la presencia de un virus informático en un sistema consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar los sectores críticos de los dispositivos de almacenamiento o los archivos ejecutables. Los programas que realizan esta tarea se denominan **chequeadores de integridad**.

Sobre la base de estas consideraciones, podemos consignar que un buen sistema antivirus debe estar compuesto por un programa detector de virus -que siempre esté residente en memoria- y un programa que verifique la integridad de los sectores críticos del disco rígido y sus archivos ejecutables. Existen productos antivirus que cubren los dos aspectos, o bien pueden combinarse productos diferentes configurados de forma que no se produzcan conflictos entre ellos.

La estructura de un programa antivirus, está compuesta por dos módulos principales: el primero denominado **de control** y el segundo denominado **de respuesta**. A su vez, cada uno de ellos se divide en varias partes:

1) **Módulo de control:** posee la técnica **verificación de integridad** que posibilita el registro de cambios en los archivos ejecutables y las zonas críticas de un disco rígido. Se trata, en definitiva, de una herramienta preventiva para mantener y controlar los componentes de información de un disco rígido que no son modificados a menos que el usuario lo requiera.

Otra opción dentro de este módulo es la **identificación de virus**, que incluye diversas técnicas para la detección de virus informáticos. Las formas más comunes de detección son el scanning y los algoritmos, como por ejemplo, los heurísticos.



Asimismo, la **identificación de código dañino** es otra de las herramientas de detección que, en este caso, busca instrucciones peligrosas incluidas en programas, para la integridad de la información del disco rígido.

Esto implica descompilar (o desensamblar) en forma automática los archivos almacenados y ubicar sentencias o grupos de instrucciones peligrosas.

Finalmente, el módulo de control también posee una **administración de recursos** para efectuar un monitoreo de las rutinas a través de las cuales se accede al hardware de la computadora (acceso a disco, etc.). De esta manera puede limitarse la acción de un programa restringiéndole el uso de estos recursos, como por ejemplo impedir el acceso a la escritura de zonas críticas del disco o evitar que se ejecuten funciones de formato del mismo.

2) **Módulo de respuesta:** la función **alarma** se encuentra incluida en todos los programas antivirus y consiste en detener la acción del sistema ante la sospecha de la presencia de un virus informático, e informar la situación a través de un aviso en pantalla.

Algunos programas antivirus ofrecen, una vez detectado un virus informático, la



posibilidad de erradicarlo. Por consiguiente, la función **reparar** se utiliza como una solución momentánea para mantener la operatividad del sistema hasta que pueda instrumentarse una solución adecuada. Por otra parte, existen dos **técnicas para evitar el contagio de entidades ejecutables**: evitar que se contagie todo el programa o prevenir que la infección se expanda más allá de un ámbito fijo.

Aunque la primera opción es la más adecuada, plantea grandes problemas de implementación.



Debido a que los virus informáticos son cada vez más sofisticados, hoy en día es difícil sospechar su presencia a través de síntomas como la pérdida de “performance” rendimiento del equipo. De todas maneras la siguiente es una lista de síntomas que pueden observarse en una computadora de la que se sospeche esté infectada por alguno de los virus más comunes:

- Operaciones de procesamiento más lentas.
- Los programas tardan más tiempo en cargarse.
- Los programas comienzan a acceder por momentos a las disqueteras y/o al disco rígido.
- Disminución no justificada del espacio disponible en el disco rígido y de la memoria RAM disponible, en forma constante o repentina.
- Aparición de programas residentes en memoria desconocidos.

La primera medida de prevención a ser tomada en cuenta es, como se dijo anteriormente, contar con un sistema antivirus y utilizarlo correctamente. Por lo tanto, la única forma de que se constituya un bloqueo eficaz para un virus es que se utilice con determinadas normas y procedimientos. Estas normas tienden a controlar la entrada de archivos al disco rígido de la computadora, lo cual se logra revisando con el antivirus todos los disquetes o medios de almacenamiento en general y, por supuesto, disminuyendo al mínimo posible todo tipo de tráfico.

Además de utilizar un sistema antivirus y controlar el tráfico de archivos al disco rígido, una forma bastante eficaz de proteger los archivos ejecutables es utilizar un programa chequeador de integridad que verifique que estos archivos no sean modificados, es decir, que mantengan su estructura. De esta manera, antes que puedan ser parasitados por un virus convencional, se impediría su accionar.



Para prevenir la infección con un **virus de sector de arranque**, lo más indicado es no dejar disquetes olvidados en la unidad de disco flexible de arranque y contar con un antivirus. Pero, además, puede aprovecharse una característica que incorpora el setup de las computadoras más modernas: variar la secuencia de arranque de la PC a "**primero disco rígido y luego unidad de disco flexible** " (C, A). De esta manera, la computadora no intentará leer la unidad de disco flexible en el arranque aunque tenga cargado un disquete.

Algunos distribuidores o representantes de programas antivirus envían muestras de los nuevos virus a los desarrolladores del producto para que los estudien o incluyan en sus nuevas versiones o upgrades, con la demora que esto implica.

En consecuencia, la detección alternativa a la de scanning y las de chequeo de actividad e integridad resultan importantes, ya que pueden detectar la presencia de un virus informático sin la necesidad de identificarlo. Y esta es la única forma disponible para el usuario de detectar virus nuevos, sean nacionales o extranjeros.

De todas maneras, existe una forma de actualizar la técnica de scanning. La misma consiste en incorporarle al antivirus un archivo conteniendo cadenas de caracteres ASCII que sean trozos de código (strings) significativos del sector vital de cada nuevo virus que todavía no esté incorporado en la base de datos del programa.

De todas formas, esta solución será parcial: la nueva cadena introducida sólo *identificará* al virus, pero no será capaz de erradicarlo.

Es muy importante que los "strings" que se vayan a incorporar al antivirus provengan de una fuente confiable ya que, de lo contrario, pueden producirse falsas alarmas o ser ineficaces. Algunos de los antivirus que soportan esta cualidad de *agregar* strings son Viruscan, F-Prot y Thunderbyte.



La NCSA (*National Computer Security Association, Asociación Nacional de Seguridad de Computadoras*) es la encargada de certificar productor antivirus. Para obtener dicha certificación los productos deben pasar una serie de rigurosas pruebas diseñadas para asegurar la adecuada protección del usuario.

Antiguamente el esquema de certificación requería que se detectara (incluyendo el número de versión) el 90 % de la librería de virus del NCSA, y fue diseñado para asegurar óptimas capacidades de detección. Pero esta metodología no era completamente eficiente.

Actualmente, el esquema de certificación enfoca la amenaza a las computadoras empresariales. Para ser certificado, el producto debe pasar las siguientes pruebas:

- a) Debe detectar el 100% de los virus encontrados comúnmente. La lista de virus comunes es actualizada periódicamente, a medida que nuevos virus son descubiertos.
- b) Deben detectar, como mínimo, el 90% de la librería de virus del NCSA (más de 6.000 virus)

Estas pruebas son realizadas con el producto ejecutándose con su configuración "por defecto".

Una vez que un producto ha sido certificado, la NCSA tratará de re-certificar el producto un mínimo de cuatro veces. Cada intento es realizado sin previo aviso al desarrollador del programa. Esta es una buena manera de asegurar que el producto satisface el criterio de certificación. Si un producto no pasa la primera o segunda prueba, su distribuidor tendrá siete días para proveer de la corrección. Si este límite de tiempo es excedido, el producto será eliminado de la lista de productos certificados. Una vez que se ha retirado la certificación a un producto la única forma



de recuperarla es que el distribuidor envíe una nueva versión completa y certificable (no se aceptará sólo una reparación de la falla).

En el caso de los virus polimórficos, se incluyen múltiples copias del virus para asegurar que el producto testeado lo detecta perfectamente. Para pasar esta prueba el antivirus debe detectar cada mutación del virus.

La A.V.P.D. (*Antivirus Product Developers, Desarrolladores de Productos Antivirus*) es una asociación formada por las principales empresas informáticas del sector, entre las que se cuentan:

- Cheyenne Software
- I. B. M.
- Intel
- McAfee Associates
- ON Technology
- Stiller Research Inc.
- S&S International
- Symantec Corp.
- ThunderByte

2.2.5 Medidas de seguridad.

En razón de lo expresado pueden extraerse algunos conceptos que pueden considerarse necesarios para tener en cuenta en materia de virus informáticos:

- No todo lo que afecte el normal funcionamiento de una computadora es un virus.
- **TODO** virus es un programa y, como tal, debe ser ejecutado para activarse.
- Es imprescindible contar con herramientas de detección y desinfección.



- **NINGÚN** sistema de seguridad es 100% seguro. Por eso todo usuario de computadoras debería tratar de implementar estrategias de seguridad antivirus, no sólo para proteger su propia información sino para no convertirse en un agente de dispersión de algo que puede producir daños graves e indiscriminados.

Para implementar tales estrategias deberían tenerse a mano los siguientes elementos:

- **Un disco de sistema protegido contra escritura y libre de virus:** Un disco que contenga el sistema operativo ejecutable (es decir, que la máquina pueda ser arrancada desde este disco) con protección contra escritura y que contenga, por lo menos, los siguientes comandos: FORMAT, FDISK, MEM y CHKDSK (o SCANDISK en versiones recientes del MS-DOS).
- **Por lo menos un programa antivirus actualizado:** Se puede considerar actualizado a un antivirus que no tiene más de tres semanas desde su fecha de creación (o de actualización del archivo de strings).
- **Una fuente de información sobre virus específicos:** Es decir, algún programa, libro o archivo de texto que contenga la descripción, síntomas y características de por lo menos los cien virus más comunes.
- **Un programa de respaldo de áreas críticas:** Algún programa que obtenga respaldo (backup) de los sectores de arranque de los disquetes y sectores de arranque maestro (MBR, Master Boot Record) de los discos rígidos. Muchos programas antivirus incluyen funciones de este tipo.
- **Lista de lugares dónde acudir:** Una buena precaución es no esperar a necesitar ayuda para comenzar a buscar quién puede ofrecerla, sino ir elaborando una agenda de direcciones, teléfonos y direcciones electrónicas de las personas y



lugares que puedan servirnos más adelante. Si se cuenta con un antivirus comercial o registrado, deberán tenerse siempre a mano los teléfonos de soporte técnico.

- **Un sistema de protección residente:** Muchos antivirus incluyen programas residentes que previenen (en cierta medida), la intrusión de virus y programas desconocidos a la computadora.
- **Tener respaldos:** Se deben tener respaldados en disco los archivos de datos más importantes, además, se recomienda respaldar todos los archivos ejecutables. Para archivos muy importantes, es bueno tener un respaldo doble, por si uno de los discos de respaldo se daña. Los respaldos también pueden hacerse en cinta (tape backup), aunque para el usuario normal es preferible hacerlo en discos, por el costo que las unidades de cinta representan.
- **Revisar todos los discos nuevos antes de utilizarlos:** Cualquier disco que no haya sido previamente utilizado debe ser revisado, inclusive los programas originales (pocas veces sucede que se distribuyan discos de programas originales infectados, pero es factible) y los que se distribuyen junto con revistas de computación.
- **Revisar todos los discos que se hayan prestado:** Cualquier disco que se haya prestado a algún amigo o compañero de trabajo, aún aquellos que sólo contengan archivos de datos, deben ser revisados antes de usarse nuevamente.
- **Revisar todos los programas que se obtengan por módem o redes:** Una de las grandes vías de contagio la constituyen Internet y los BBS, sistemas en los cuales es común la transferencia de archivos, pero no siempre se sabe desde dónde se está recibiendo información.



- **Revisar periódicamente la computadora:** Se puede considerar que una buena frecuencia de análisis es, por lo menos, mensual.

Finalmente, es importante tener en cuenta estas sugerencias referentes al comportamiento a tener en cuenta frente a diferentes situaciones:

- Cuando se va a revisar o desinfectar una computadora, es conveniente apagarla por más de 5 segundos y arrancar desde un disco con sistema, libre de virus y protegido contra escritura, para eliminar virus residentes en memoria. No se deberá ejecutar ningún programa del disco rígido, sino que el antivirus deberá estar en el disquete. De esta manera, existe la posibilidad de detectar virus stealth.
- Cuando un sector de arranque (boot sector) o de arranque maestro (MBR) ha sido infectado, es preferible restaurar el sector desde algún respaldo, puesto que en ocasiones, los sectores de arranque genéricos utilizados por los antivirus no son perfectamente compatibles con el sistema operativo instalado. Además, los virus no siempre dejan un respaldo del sector original donde el antivirus espera encontrarlo.
- Antes de restaurar los respaldos es importante no olvidar apagar la computadora por más de cinco segundos y arrancar desde el disco libre de virus.
- Cuando se encuentran archivos infectados, es preferible borrarlos y restaurarlos desde respaldos, aún cuando el programa antivirus que usemos pueda desinfectar los archivos. Esto es porque no existe seguridad sobre si el virus detectado es el mismo para el cual fueron diseñadas las rutinas de desinfección del antivirus, o es una mutación del original.



- Cuando se va a formatear un disco rígido para eliminar algún virus, debe recordarse apagar la máquina por más de cinco segundos y posteriormente arrancar el sistema desde nuestro disquete limpio, donde también debe encontrarse el programa que se utilizará para dar formato al disco.
- Cuando, por alguna causa, no se puede erradicar un virus, deberá buscarse la asesoría de un experto directamente pues, si se pidiera ayuda a cualquier aficionado, se correrá el riesgo de perder definitivamente datos si el procedimiento sugerido no es correcto.
- Cuando se ha detectado y erradicado un virus es conveniente reportar la infección a algún experto, grupo de investigadores de virus, soporte técnico de programas antivirus, etc. Esto que en principio parecería innecesario, ayuda a mantener estadísticas, rastrear focos de infección e identificar nuevos virus, lo cual en definitiva, termina beneficiando al usuario mismo.

Para concluir debes de tener en cuenta la siguiente información de referente a los sistemas operativos Microsoft Windows en sus diferentes versiones, ya que la información que Microsoft posee sobre seguridad y protección de los equipos ocuparía varios volúmenes en una enciclopedia. Sin embargo, y con clara intención de hacer las cosas más sencillas, he resumido en tres pasos lo que debes hacer para que tu equipo esté protegido. Desde aquí te aconsejo encarecidamente que consideres “sagrados” estos pasos y no dejes de tenerlos presentes.

1.- Utiliza un servidor de seguridad (Firewall). Antes de conectar tu equipo a Internet, debes instalar un servidor de seguridad. Es un software o hardware que ayuda a proteger tu PC de hackers y muchos tipos de virus y gusanos informáticos. Si dispones, por ejemplo, del sistema operativo Microsoft Windows® XP, utiliza el Servidor de seguridad de conexión a Internet integrado.



2.- Mantén tu software actualizado. Cuando adquieres software original tienes derecho a las actualizaciones del mismo. Éstas se realizan de manera muy sencilla, o incluso automáticamente, como sucede en Microsoft Windows® XP.



3.- Utiliza un software antivirus actualizado. Un software antivirus es un programa que el equipo ya tiene instalado como versión demo o versión completa, o que se adquiere y se instala después. Te ayuda a proteger tu equipo contra los virus, gusanos, troyanos y otros invasores no deseados, que pueden hacer "enfermar" a su



equipo. Hay muchos en el mercado y seguramente los conoce (Panda, Symantec, McAfee, Avast!, NOD32, etc)



ANEXO 2 Removiendo virus de una computadora.

Recordemos que algunos virus que se han apoderado de nuestra computadora, tienden a infectar algunas partes esenciales de cualquier sistema operativo. Así que es necesario aprender la técnica con la cual podemos erradicar la infección sin que se vea afectado nuestro equipo. En éste caso utilizaremos Windows XP SP2 y utilizaremos los programas Norton Antivirus 2004 y Avast! 4.6 Profesional, los pasos son los mismos para cualquier otro Sistema Operativo y antivirus.

1. Iniciar Windows en Modo seguro:

- a) Inicie Windows o si se está ejecutando, cierre la sesión y apague el equipo.
- b) Reinicie el equipo. El equipo inicia ejecutando un conjunto de instrucciones conocidas como funciones básicas de entrada/salida (BIOS del inglés Basic Input/Output System.) Las pantallas que se presenten, dependen del fabricante del BIOS. Algunos equipos muestran una barra de progreso del



BIOS, en tanto que otros equipos, puede que no muestren alguna indicación durante este proceso.

- c) Tan pronto termine la carga del BIOS, comience a presionar la tecla F8 en su teclado. Haga esto hasta que se presente el menú de Opciones avanzadas de Windows.

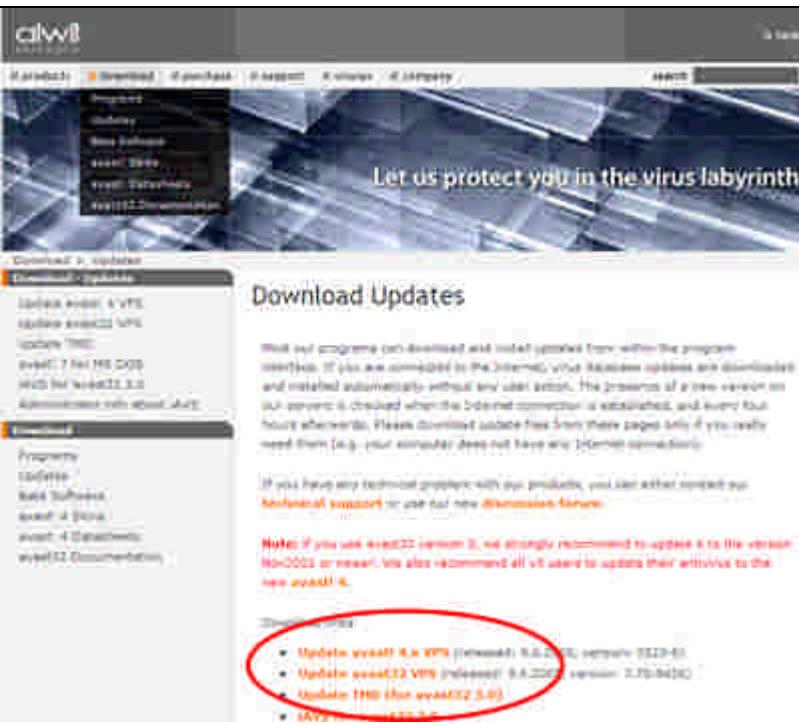
Nota: Si presiona la tecla F8 demasiado rápido, algunos equipos arrojarán un mensaje de "error de teclado." Por favor reinicie e intente de nuevo.

- d) Mediante las flechas del teclado, desplácese y seleccione la **opción Modo seguro sin acceso a Red** y presione la tecla Intro.
- e) Si la computadora está conectada a alguna red privada, te sugiero que la desconectes.

2. Actualización del programa Antivirus.

Desde una segunda máquina, que sepamos que no está infectada, nos tenemos que conectar a la página Web del programa antivirus, con la finalidad de descargar la última base de datos de Virus, recordemos que de nada sirve nuestro Antivirus si no está actualizado. Todos los antivirus ofrecen la opción de actualizar el motor de búsqueda del antivirus mediante la descarga de un archivo que después se tiene que instalar dentro de la computadora que vamos a limpiar.



	<p>Norton Antivirus 2004</p> <p>Página Web</p> <p>http://www.symantec.com</p>
	<p>Avast! 4.6 Profesional</p> <p>Página Web</p> <p>http://www.avast.com/</p>

Descargamos las actualizaciones de la última fecha disponible. Y debemos de guardar el archivo en algún medio ya sea CD, Floppy, o dispositivo de almacenamiento USB (todo va a depender del tamaño del archivo de actualización), para poder transportarlo a la computadora infectada.

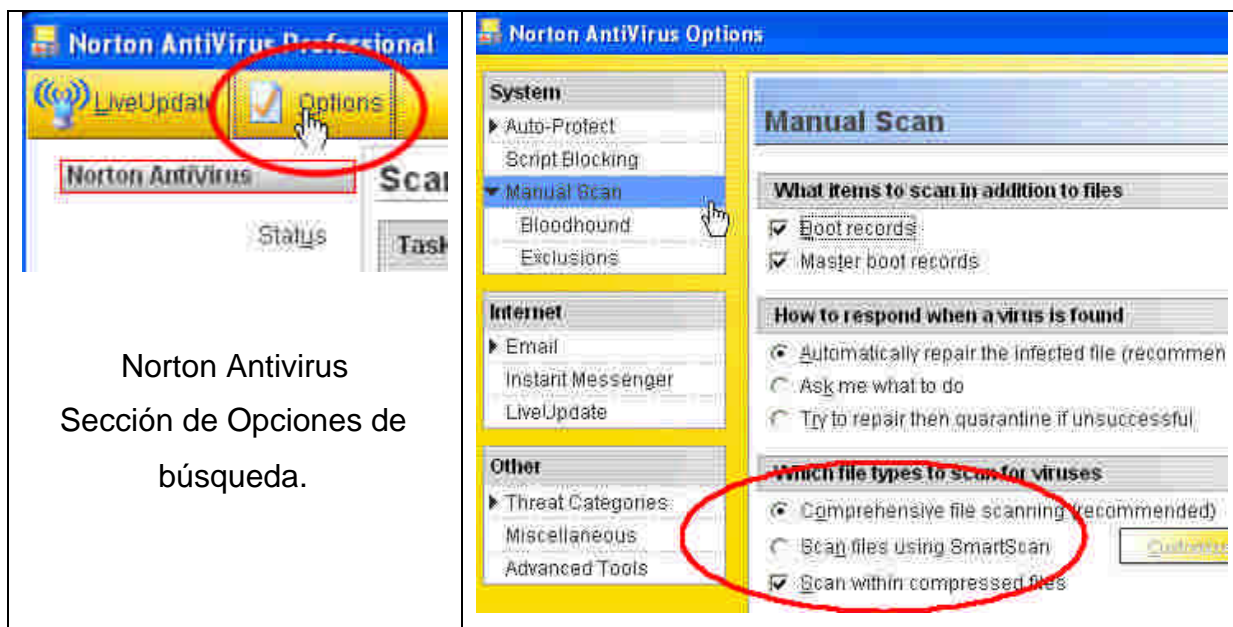


3. Instalado actualizaciones

Una vez que tenemos las actualizaciones en el medio, las debemos de instalar en la computadora, en el caso de Norton Antivirus y de Avast! 4.x las actualizaciones vienen en archivos ejecutables. Esto quiere decir que solo debemos de dar doble clic y seguir los pasos que aparezcan en la pantalla. Al finalizar de actualizar es recomendable reiniciar la computadora y volver a hacer los pasos 1.

4. En busca de virus

Una vez que la computadora se haya reiniciado, debemos de arrancar nuestro programa antivirus dentro de las opciones hay que pedir que haga una búsqueda hasta en los archivos compresos y que automáticamente trate de reparar el archivo si se encuentra un virus de lo contrario la mandará a quarentena.





		<p>Avast! 4.6 Profesional Sección de Opciones de búsqueda</p>

Una vez puesta la opción de búsqueda en archivos compresos, y que responda automáticamente, debemos iniciar la búsqueda en todos los discos de la computadora. El tiempo va a depender de la cantidad de archivos en la computadora y del tamaño de los discos.

Al finalizar la búsqueda se entrega un reporte sobre el estado de la computadora, en caso de que no se haya podido eliminar un virus de la computadora, te sugiero que apuntes el nombre con el que identifica al virus (ejem. W32.Nimda.enc) y en la página de los antivirus busca si hay herramientas destinadas para remover



específicamente ese tipo de virus. Habrá que descargar desde otra computadora la aplicación necesaria para poder remover la infección. En caso de que no exista en cualquier buscador puedes ingresar el nombre del virus junto con la palabra remover para que te busque información sobre como quitar la infección.

5. Reiniciando

En caso de que tu computadora haya mostrado resultados de infección te sugiero que reinicies al finalizar el proceso de limpieza y vuelvas a hacer una segunda búsqueda. Con el fin de quedar satisfechos con la computadora.

Spyware.

1. ¿Qué es el spyware?

El spyware es un software que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario de la misma.

El término spyware **también se utiliza** más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up o ventanas emergentes), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.





Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.

Sin embargo, a **diferencia de los virus**, no se intenta replicar en otros ordenadores, por lo que funciona como un parásito.

Las **consecuencias de una infección** de spyware moderada o severa (a parte de las cuestiones de privacidad) generalmente incluyen una pérdida considerable del rendimiento del sistema (hasta un 50% en casos extremos), y problemas de estabilidad graves (el ordenador se queda "colgado"). También causan dificultad a la de conectar a Internet.



hora

2. Programas antispyware

En Internet existe un sin fin de herramientas para remover el spyware, los hay desde los programas no comerciales hasta los programas con licencias de uso.

Software NO comercial	Software comercial
Ad-Aware SE Personal Edition 1.06	Webroot Spy Sweeper 4.0
Spybot - Search & Destroy 1.4	SpyHunter 2.0.1086
Spyware Doctor 3.2	Spyware Eliminator
SpywareBlaster 3.4	CounterSpy
Bazooka Adware and Spyware Scanner	PestPatrol
Microsoft Windows AntiSpyware	Ad-aware Pro



En caso de que no cuentes con un programa antispymware te recomiendo que visites la página <http://www.download.com> y busques alguno de la lista de software libre.



3. Cómo remover spyware

Como en el caso de los virus, el spyware se apropia de los recursos del sistema operativo, por lo que al removerlos corremos el riesgo de que perdamos la conectividad a Internet o el falló en alguna aplicación. Por lo que necesitamos hacer la limpieza de spyware sin arrancar al 100% el sistema operativo y para esto tenemos que **Iniciar Windows en Modo seguro (ver punto 1 del Anexo 2)**,

Una vez iniciado en modo seguro procedemos a realizar la búsqueda de spyware con las opciones de fabrica o de preferencia que la primer búsqueda sea profunda o completa. Es necesario recordar que día a día hay nuevos spyware por lo que hay que mantener al día nuestro programa antispymware. Y por recomendación hay que dejar que el programa remueva todo lo que sea spyware.



El riesgo de quitar el spyware de la computadora como ya lo mencione, es quedarnos sin los protocolos para conectarnos en red o a Internet, por lo que debemos de parchar o reinstalar solo esas opciones de los protocolos. Para obtener el archivo para la corrección de éste problema envía un



correo a wmaster@fcaenlinea.unam.mx junto con el sistema operativo que tienes para poder enviarte el parche adecuado. O si lo prefieres documéntate sobre los problemas del Winsock al remover spyware.





Unidad 3.

Topología de redes

- 2.1 En canal
- 2.2 En anillo
- 2.3 En estrella





Objetivos particulares de la unidad

Al culminar el aprendizaje de la unidad lograras identificar la topología de las redes LAN y señalar sus características principales, así como sus ventajas y desventajas.





3. Topologías

Los diferentes componentes que van a formar una red se pueden interconectar o unir de diferentes maneras, siendo la forma seleccionada un factor determinante del rendimiento y funcionalidad de la red.

La disposición de los diferentes componentes de una red se conoce con el nombre de topología de red. La topología que se seleccione para una red dependerá de diferentes factores, como:

- El número de computadoras
- La cantidad de cableado requerido
- La facilidad de la instalación
- La forma y velocidad con que viajan los datos en la red
- La facilidad para detectar y reparar las fallas que se puedan producir, etc.

Puede ser que una red se forme con la unión de más de una topología, a esta unión de varias topologías, se le conoce como topología híbrida y requiere de software y hardware como: dispositivos centrales (hub), puentes (bridges), ruteadores (routers) o puertas de enlace (gateways),

Cuando se selecciona la topología que va a tener una red, se deben considerar dos aspectos importantes:

1. La topología física o la disposición real de los componentes de la red, y
2. La topología lógica o arquitectura de la red, que es la forma en que las máquinas se comunican dentro de la red.

3.1 En canal.

La topología en canal o de bus tiene todos sus nodos conectados directamente a un cable central y lineal. Físicamente cada dispositivo (computadora, impresora, escáner, etc.) está conectado a un cable común. El cable o canal propaga las



señales en ambas direcciones, de manera que todos los dispositivos puedan ver todas las señales de todos los demás dispositivos. Esta característica puede ser ventajosa si se requiere que todos los dispositivos obtengan esa información, pero podría representar una desventaja debido al tráfico y podrían presentarse colisiones que afecten a la red.

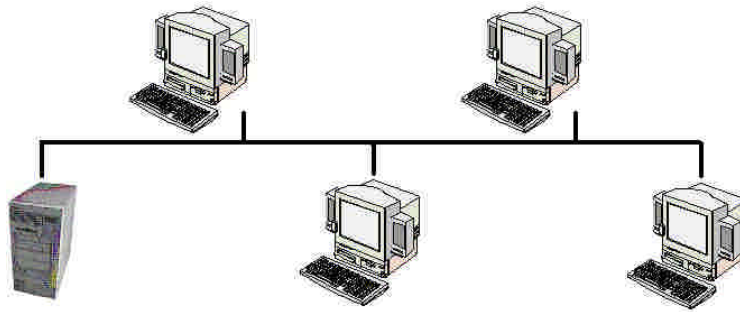


Fig. 3.1 Topología en canal o bus

Las ventajas de la topología en canal o bus son:

- La facilidad de incorporar o quitar dispositivos de la red.
- Se requiere una menor cantidad de cableado que en otras topologías.

Su principal desventaja es:

- La ruptura del cableado hace que se rompa toda la comunicación dentro de la red.

3.2 En anillo.

Una topología en anillo se caracteriza por conectar secuencialmente en un cable todos los dispositivos (computadoras, impresora, escáner, etc.) formando un anillo cerrado, en el que cada dispositivo o nodo está conectado solamente con los dos dispositivos o nodos adyacentes.

Para que la señal pueda circular, cada dispositivo o nodo debe transferir la señal al nodo adyacente.

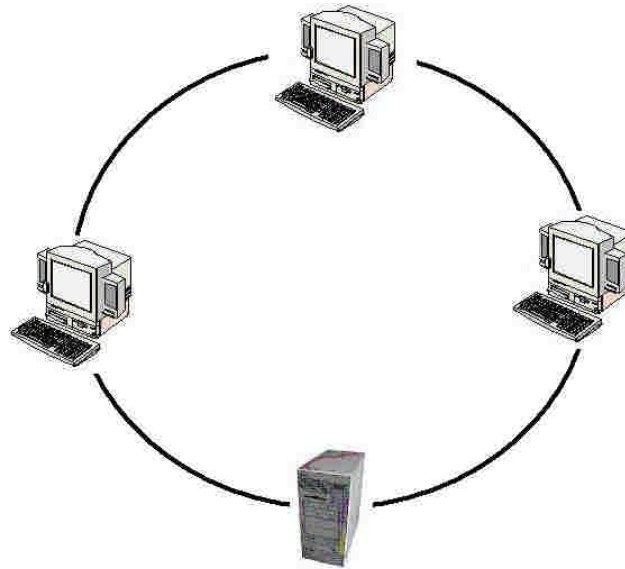


Fig. 3.2 Topología en anillo.

Es posible establecer una red con topología en anillo doble. Esta topología consta de dos anillos concéntricos, donde cada dispositivo de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí.

Esta topología es análoga a la topología de anillo, con la diferencia de que, para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante, que conecta los mismos dispositivos.

En una red con esta topología, cada dispositivo o nodo, examina la información enviada a través del anillo, si la información no está dirigida a ese nodo, la entrega al siguiente nodo del anillo, y así, el proceso se repite hasta que la señal llega al nodo destino.

La principal ventaja en redes con topología en anillo, es la estabilidad con respecto al tiempo que tardan las señales en llegar a su destino, sin que se presenten colisiones.



La desventaja que tiene esta topología es que la ruptura en la conexión de un dispositivo, tira toda la red.

3.3 En estrella.

La topología en estrella consta de un dispositivo central llamado concentrador o hub, desde el cual se irradian todos los enlaces hacia los demás dispositivos o nodos. Por este concentrador o hub, pasan todas las señales que circulan en la red. La función principal del hub, es agilizar la transmisión de señales y evitar colisiones.

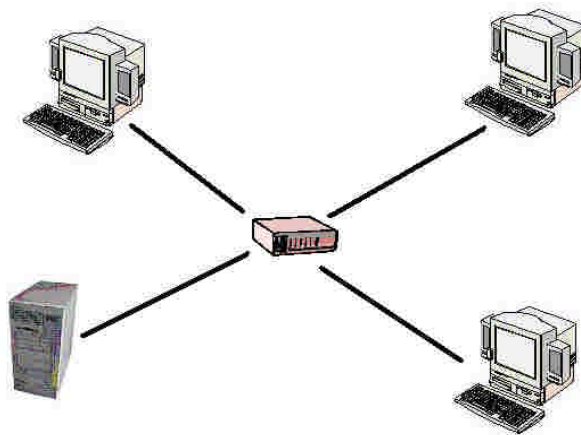


Fig. 3.3 Topología en estrella.

Las ventajas de la topología en estrella son:

- Facilidad para incorporar o eliminar dispositivos de la red.
- La ruptura del cableado de un dispositivo, solo afecta a éste.
- Se detecta con facilidad alguna desconexión.

Las desventajas que presenta, son las siguientes:

- La cantidad de cableado requerido es superior a cualquier otra topología.
- La adquisición del hub, incrementa el costo de instalación.
- Una falla en el hub, afecta a toda la red.



Topologías híbridas

El canal, la estrella y el anillo se pueden combinar para formar topologías híbridas.

La topología híbrida anillo – estrella, consiste físicamente en una estrella centralizada en un concentrador, mientras que a nivel lógico, la red funciona como un anillo.

La topología híbrida canal – estrella es un canal o bus que se cablea físicamente como una estrella mediante concentradores, es decir consiste en la unión de dos o más redes con topología en estrella unidas mediante un cable lineal central que utiliza la topología en canal.

En esta topología, la señal generada por un dispositivo, es enviada al concentrador, el cuál la transmite al otro hub, conectado en el canal, y de este concentrador llega al dispositivo destino.

Topología en estrella jerárquica.

Mediante concentradores dispuestos en cascada, se interconectan redes con diferentes topologías, para formar una red jerárquica.

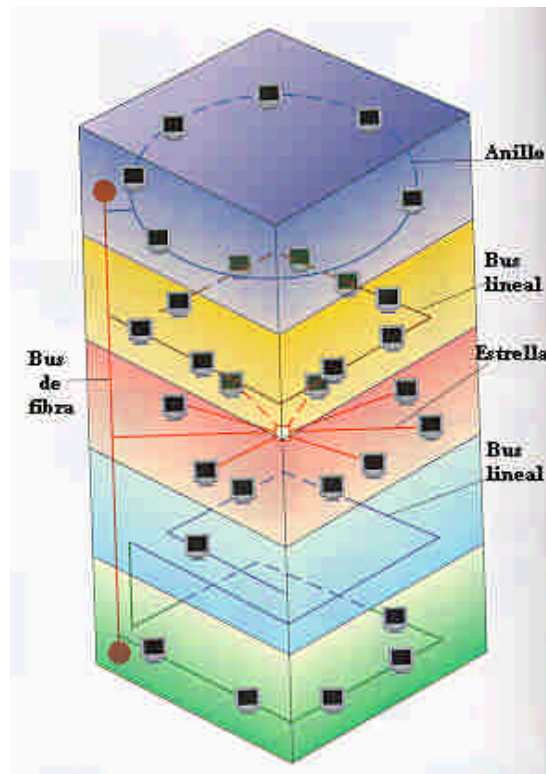


Fig. 3.4 Topología en estrella jerárquica.

Arquitectura de red.

La arquitectura de una red es el estándar que define la manera en que se lleva a cabo la transmisión de las señales eléctricas. Estas arquitecturas fueron creadas por los fabricantes de las tarjetas de red y los medios o cableado requerido.

Las arquitecturas mas comunes son: Ethernet y Token Ring.

La arquitectura Token Ring, se aplica en redes con topología anillo – estrella, el cableado está dispuesto en forma de estrella, pero las señales viajan en forma de anillo. Cuando una computadora realiza una transmisión de datos a otra, debe esperar un permiso llamado token (testigo). Este permiso, pasa de dispositivo en dispositivo hasta llegar a alguno que requiere efectuar una transmisión. Cuando sucede esto, es incorporado al testigo la dirección del dispositivo emisor, la dirección



del dispositivo receptor y los datos que se van a enviar, y así, va pasando de dispositivo en dispositivo hasta llegar a su destino.

La arquitectura Eternet, puede usarse en redes con topologías en Canal, estrella y canal – estrella. Esta arquitectura se basa en las siguientes premisas:

- Todos los dispositivos tienen el mismo derecho, posibilidad o prioridad de transmitir paquetes o grupos de datos.
- Para poder transmitir, deberán “escuchar” hasta el momento en que ningún dispositivo este realizando una transmisión, y entonces podrá hacerlo.
- Controlar que mientras este realizando una transmisión, ningún otro dispositivo intente transmitir algo para evita que se produzca una colisión.

Existen diversas maneras de establecer una red; estas dependen de la topología y la arquitectura seleccionadas, la posibilidad de crecimiento o expansión y actualización y la velocidad que se requiera para efectuar transmisiones.





Unidad 4. Graficadores, manejo y aplicación

- 4.1 Introducción.
- 4.2 Manejo de texto.
- 4.3 Elaboración de gráficas.
 - 4.3.1 Sectores.
 - 4.3.2 Barras.
 - 4.3.3 Áreas.





Objetivos particulares de la unidad

El alumno aprenderá los conceptos básicos para la elaboración de graficas, tanto bidimensionales como tridimensionales, utilizando los datos de la hoja de calculo de Microsoft Excel. Esto le permitirá poder realizar representaciones visuales de información relevante para las organizaciones.





Introducción

Los gráficos resultan muy útiles cuando se desea representar el cambio de una serie de valores a través del tiempo.

Excel cuenta con las herramientas necesarias para la creación de gráficos de distintos tipos, como gráficos de barras, circulares, de pastel, etcétera.

Siendo una hoja de cálculo permite utilizar los datos contenidos en las celdas para el desarrollo de un gráfico. Excel utiliza un asistente para gráficos que ayuda al usuario la creación de un gráfico.

Los pasos necesarios para la creación de un gráfico son los siguientes:

Paso 1

Suponiendo que tenemos los siguientes datos en una hoja de Excel.

PRODUCTO	PRECIO	CANTIDAD
Tenis para correr	\$ 800.00	34
Tenis casual	\$ 1,000.00	56
Tenis para básquetbol	\$ 1,200.00	45
Tenis para voleibol	\$ 900.00	21
Tenis cross training	\$ 750.00	78
Tenis de fútbol	\$ 600.00	105

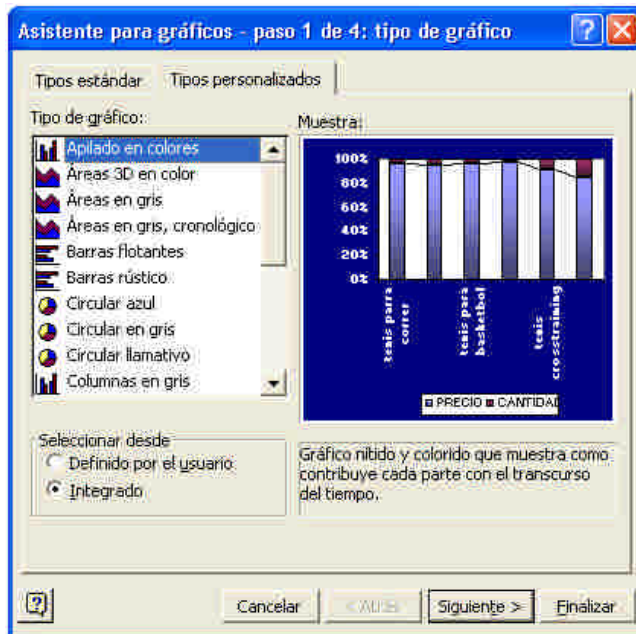
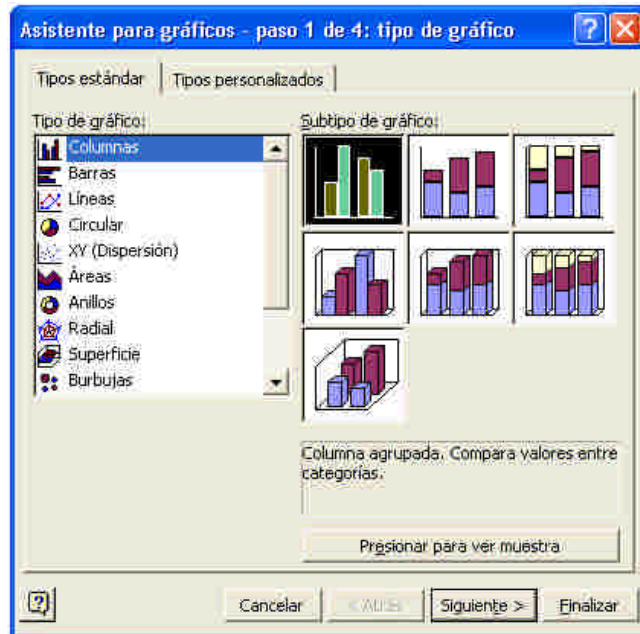
Se debe seleccionar con el ratón o el teclado un conjunto de celdas.

Posteriormente se presiona el botón de *Asistente para gráficos* que se encuentra en la barra de herramientas.



PASO 1

Entonces aparece la siguiente ventana:
Aquí, se puede seleccionar un tipo de gráfico, en este caso está señalado el tipo de gráfico de columna y un subtipo de columna agrupada. Si se mantiene presionado el botón de *Presionar para ver muestra* aparecerá la muestra del gráfico con los datos.



También se pueden seleccionar los *Tipos Personalizados*, como se muestra en la ventana de la izquierda.

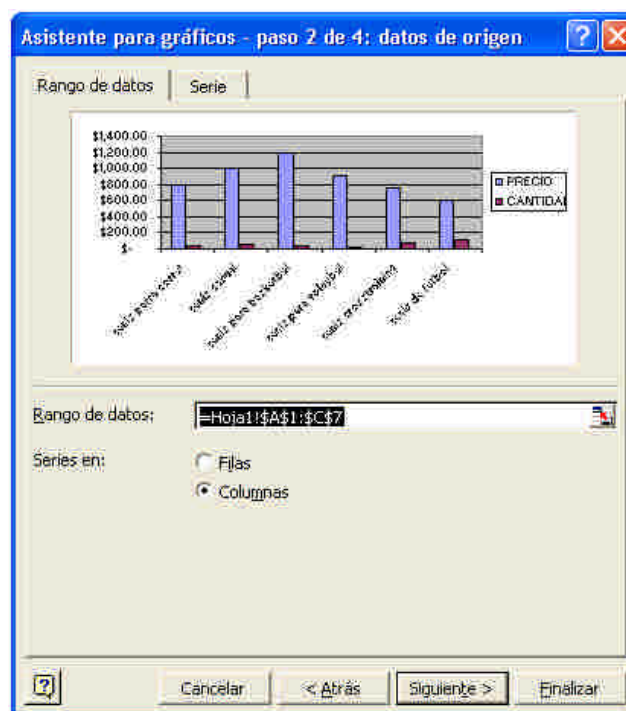
El tipo de gráfico personalizado, corresponde al tipo de gráfico creado por el usuario.

Una vez seleccionadas las opciones correspondientes se presiona el botón de *Siguiente*.



PASO 2

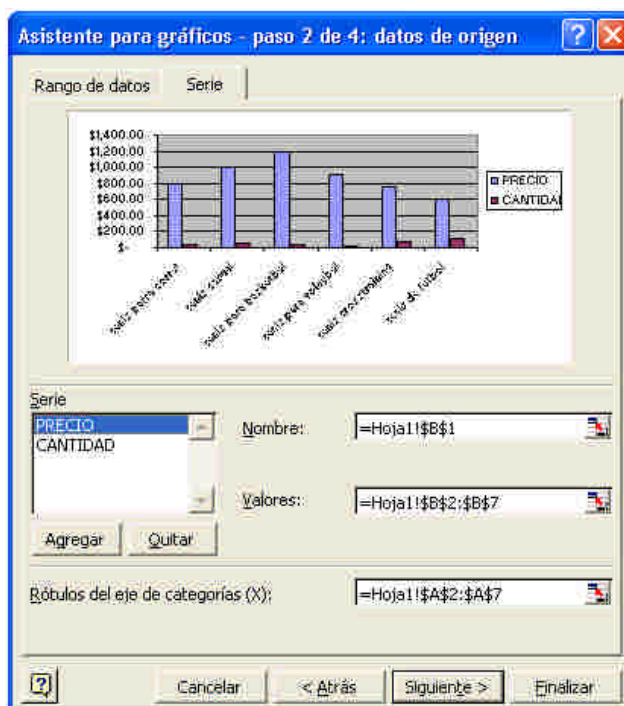
Se presenta la siguiente ventana:



En esta parte se le indica al Asistente que datos se incluyen en el gráfico, además de cómo se deben presentar las series, si en *Filas* o en *Columnas*.

En la pestaña de *Serie*:

Se determina el nombre y rango de cada serie, el cual puede ser modificado, se pueden agregar mas series o eliminarlas, y por último se pueden modificar los rótulos del eje de las categorías.





Si la hoja de Excel no incluye los títulos de cada columna, Excel utiliza el nombre de serie 1, serie 2, serie 3 etcétera. En el caso de este ejemplo si se incluyeron los nombres de cada columna.

Entonces se presiona el botón de *Siguiente*

PASO 3

Aparece una ventana con las opciones del gráfico, el cual tiene 6 pestañas:

- Títulos
- Eje
- Líneas de división
- Leyenda
- Rótulos de datos
- Tabla de datos



Títulos:

En esta opción se le puede dar un título al gráfico y una descripción para cada eje de valores.

Eje:

Aquí se presentan una serie de casillas de verificación que corresponden a cada eje.



La escala temporal esta disponible en gráficos de líneas, columnas, barras y áreas bidimensionales y tridimensionales.

Líneas de división:

Son líneas verticales y horizontales que ayudan a ver el gráfico de una manera mas clara. Al seleccionar esta pestaña se pueden visualizar o no dichas líneas.

Leyenda:

Excel presenta una leyenda en la parte derecha del grafico. Es posible visualizar u ocultar la leyenda y en caso de que se visualizada existen 5 opciones para su visualización.

- Abajo
- Esquina
- Arriba
- Derecha
- Izquierda.

Rótulos de datos:

Un grafico por sectores circulares se identifica por porcentaje. Un grafico de columnas, un grafico de líneas puede tener rótulos indicando el valor de cada punto y así sucesivamente. Se pueden visualizar o no los rótulos.

Por ultimo el cuadro dialogo contiene una opción para añadir la clave de leyenda junto a rotulo.

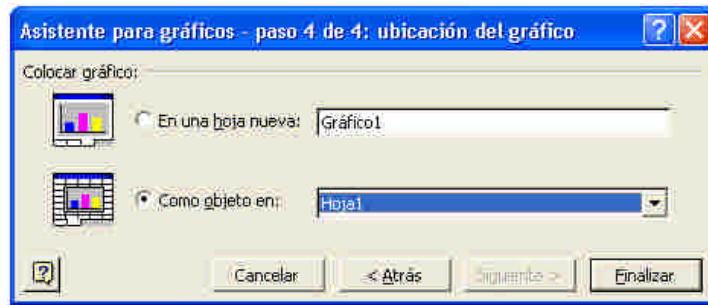
Tabla de datos:

Esta pestaña, permite activar la opción de *Mostrar tabla de datos*, con los valores representados en el grafico, y una segunda opción para *Mostrar clave de leyenda*.

Por ultimo se presiona el botón de Siguiente

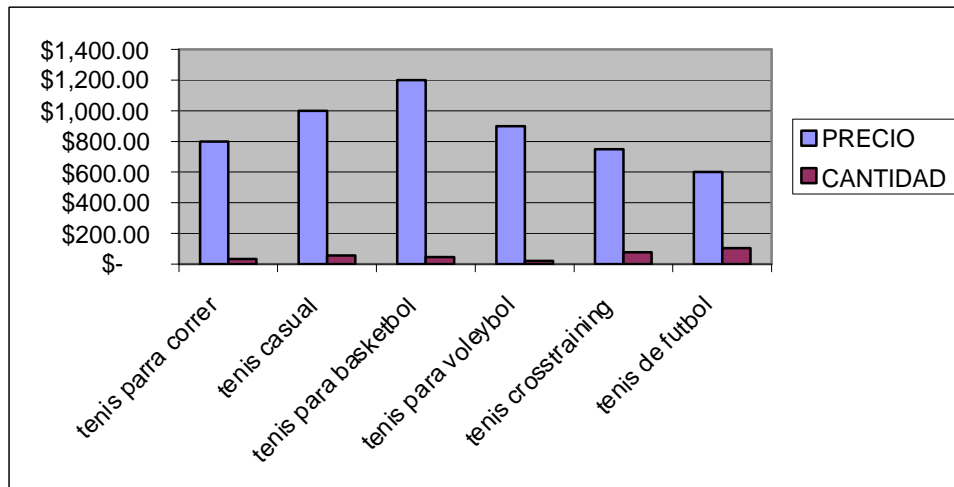
PASO 4

A continuación se muestra la última ventana del asistente :



Si se desea que el gráfico aparezca en una hoja de datos, se selecciona la opción *Como objeto en*, o se puede escoger la opción de pegarlo *En una hoja nueva*.

El resultado es un gráfico con esta apariencia:





Unidad 5. Herramientas de presentación, manejo y aplicación

- 5.1 Qué es una presentación.
- 5.2 Creación de una presentación.
- 5.3 Creación del aspecto de una presentación.
- 5.4 Patrón de diapositivas.
- 5.5 Plantillas.
- 5.6 Imágenes.
- 5.7 Formato de texto.
- 5.8 Impresión de presentaciones.
- 5.9 Ecuaciones, tablas y gráficas en una presentación.
- 5.10 Presentaciones electrónicas.
 - 5.10.1 Ejecución y control de una presentación.





Objetivos particulares de la unidad

Al finalizar la presente unidad conocerás el manejo de las principales herramientas para crear una presentación electrónica con *Microsoft Office XP PowerPoint*, serás capaz de dar formato, movimiento, estilos, insertar imágenes, sonidos, tiempos y muchas otras funciones básicas como abrir, modificar, publicar e imprimir una presentación.

El alumno estará en posibilidad de realizar presentaciones electrónicas profesionales.





5. Herramientas de presentación, manejo y aplicación.

Existen en la actualidad diversos software destinados a la elaboración de presentaciones electrónicas como: PowerPoint, Freelance o Harvard Graphics. Para esta unidad trabajaremos con *PowerPoint XP 2003*, esta última versión incluye nuevas herramientas destinadas a facilitar y automatizar la forma de trabajo para crear, presentar y colaborar en presentaciones que logren un mayor impacto.

Como bien sabes para esta quinta unidad debes adquirir los conocimientos necesarios para crear presentaciones electrónicas, con la ayuda de *PowerPoint XP 2003*, un programa sencillo y por lo tanto fácil de utilizar. Esta nueva versión te permite ver presentaciones completas creadas desde las versiones anteriores como *PowerPoint 97* y versiones posteriores. El visor de esta versión también permite abrir presentaciones de *Microsoft PowerPoint* protegidas con contraseña. Con *PowerPoint Viewer 2003* podrás ver e imprimir presentaciones, pero no podrás modificarlas.



Este visor no admite las siguientes características de *Microsoft PowerPoint*:

- Presentaciones de Information Rights Management (IRM).
- Ejecutar macros o programas; abrir objetos vinculados o incrustados.

Los requisitos del sistema son los siguientes:

- Sistemas operativos compatibles: Windows 2000 Service Pack 3, Windows 98, Windows 98 Second Edition, Windows Server 2003, Windows XP
- Esta descarga funciona con presentaciones creadas en los siguientes programas de Office:
 - Microsoft Office PowerPoint 2003
 - Microsoft PowerPoint 2002



- Microsoft PowerPoint 2000
- Microsoft PowerPoint 97

La interfaz

Para comenzar es necesario que conozcas la interfaz del programa con el que hemos de trabajar, como ya te habíamos mencionado en la Guía de Estudios, es una interfaz muy parecida a *Word* y *Excel* (programa con los cuales tuviste un acercamiento importante el semestre pasado) debido a que pertenecen a la misma familia “*Microsoft Office*”, esto te facilitará el trabajo.

Es de suma importancia que reconozcas los elementos básicos de la interfaz como son: la pantalla, las barras y áreas de trabajo, etc, para que te vayas familiarizando con el entorno. A continuación te presentamos, la pantalla principal (*Fig 1*) con la descripción de cada una de sus partes, es necesario que te aprendas cómo se llaman, donde están y para qué sirven, ya que esto te ayudará a elaborar los ejercicios y las presentaciones de manera más eficaz y rápida.

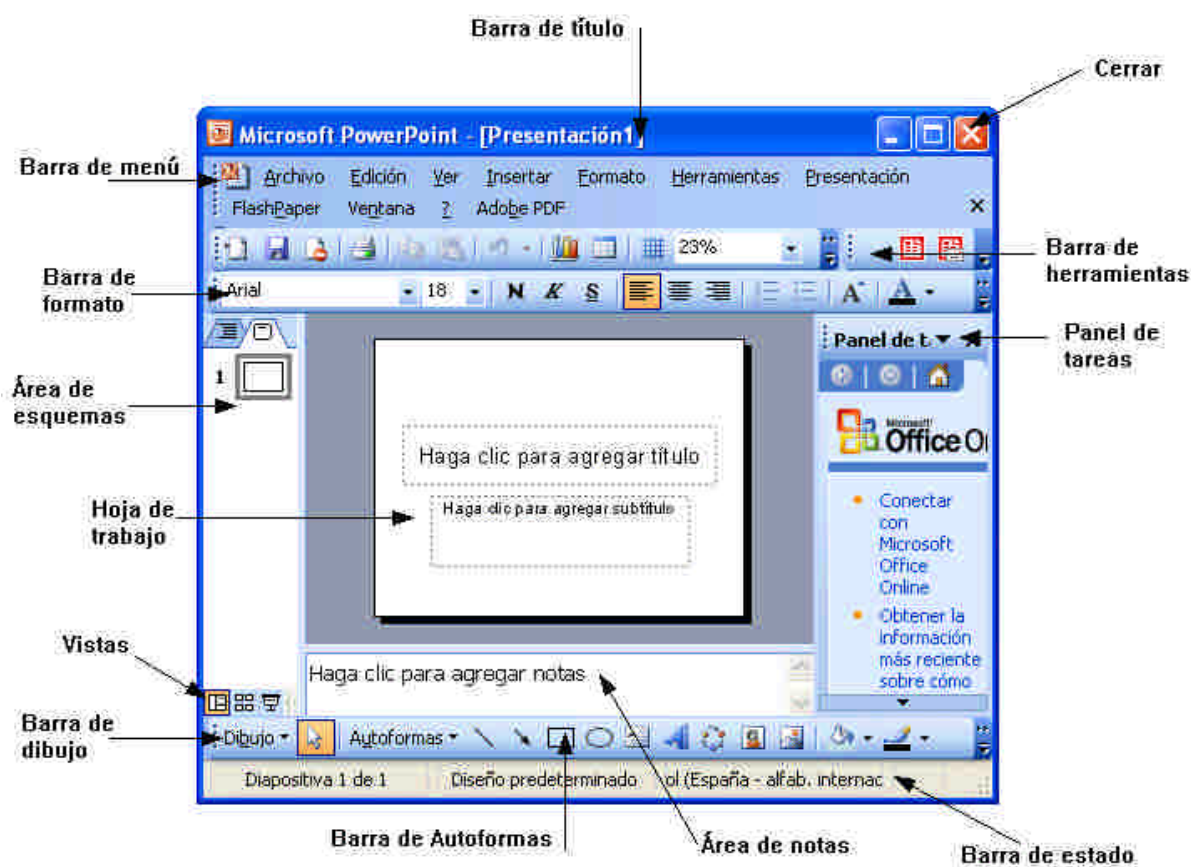


Fig 1



5.1 Qué es una presentación

Definición según la *Real lengua española*: Manifestación, exposición, proposición.

Una presentación electrónica comúnmente utilizada en exposiciones orales es un documento que le sirve de apoyo al orador o ponente en su exposición, le ayuda como soporte y secuencia a la hora de la explicación. Además de que *PowerPoint* le da la facilidad de integrar diferentes elementos como: esquemas, texto, imágenes estáticas o animadas, ligas a Internet u a otros documentos de ppt, video, audio, entre otros medios de interacción, que beneficiarán la presentación.

Una presentación es la agrupación de varias diapositivas en un archivo, de manera que se pueda ir mostrando una de tras de la otra *Fig 2*. Con éstas se logra una secuencia lógica de texto e imágenes, con ciertos intervalos de tiempo (determinado o indeterminado), también se pueden utilizar efectos de animación o transición, que le permiten ejemplificar de mejor manera y acompañar las palabras del orador.



Fig 2



5.2 Creación de una presentación.

Para la creación de una presentación electrónica el usuario podrá elegir entre las cuatro formas existentes, las cuales mencionaremos de manera general y que podrás encontrar en el panel derecho de tu computadora con el título de “*Nueva presentación*”.¹



Presentación en blanco

Presentación en blanco, esta opción posiblemente es de las más utilizadas, habré una nueva presentación sin ningún diseño, ni contenido predefinido, el usuario se encarga de elegir las características de tipografía, tipo de fondo sólido o texturizado y combinaciones posibles de colores necesarios para su presentación. *Fig 3*



A partir de una plantilla de diseño

A partir de una plantilla de diseño, puedes crear una presentación con la ayuda de algunas plantillas que ya tiene predefinidas el programa, las cuales proporcionan combinaciones de fondo, color y fuente de tipografía, profesionalmente elegidas para que no tengas que preocuparte por elegir los tonos adecuados.

Estas combinaciones permitirán siempre la buena lectura debido al contraste utilizado entre el fondo y la tipografía. *Fig 4*




A partir de una presentación existente...


A partir de una presentación existente; crea una presentación siguiendo el formato de alguna que hayas realizado anteriormente.

¹ Te recomendamos revises las lecturas propuestas en las lecturas sugeridas para un mayor conocimiento de ellas.



 A partir del Asistente para autocontenido...

Asistente de autocontenido, para este tipo de presentaciones el programa te proporciona por tema varias diapositivas prediseñadas. Al elegir esta opción se abre una ventana emergente *Fig 5* donde le va solicitando al usuario llenar algunos campos para ir personalizando el tipo de presentación deseada.

 <i>Fig 3</i>	<i>Presentación en blanco</i>
<i>A partir de una plantilla de diseño</i>	 <i>Fig 4</i>

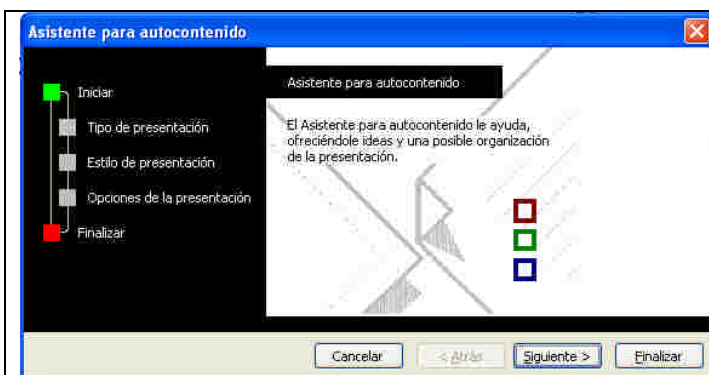


Fig 5

Asistente de autocontenido

Para las cuatro formas diferentes que existen al crear una presentación se les pueden aplicar plantillas de diseño. Existen 27 diseños predefinidos, basta con solo dar doble clic al que se desee usar y se aplicará a todas las diapositivas que hayas elaborado. Al aplicar un diseño diferente, tanto los textos como los objetos permanecen en la diapositiva sin cambios, aunque posiblemente necesitarán ser reordenados para ajustarse al nuevo diseño.

PowerPoint te permite cambiar la apariencia de la presentación en cualquier momento; es decir, formato, colores, tamaño, tiempos, animaciones, etc.

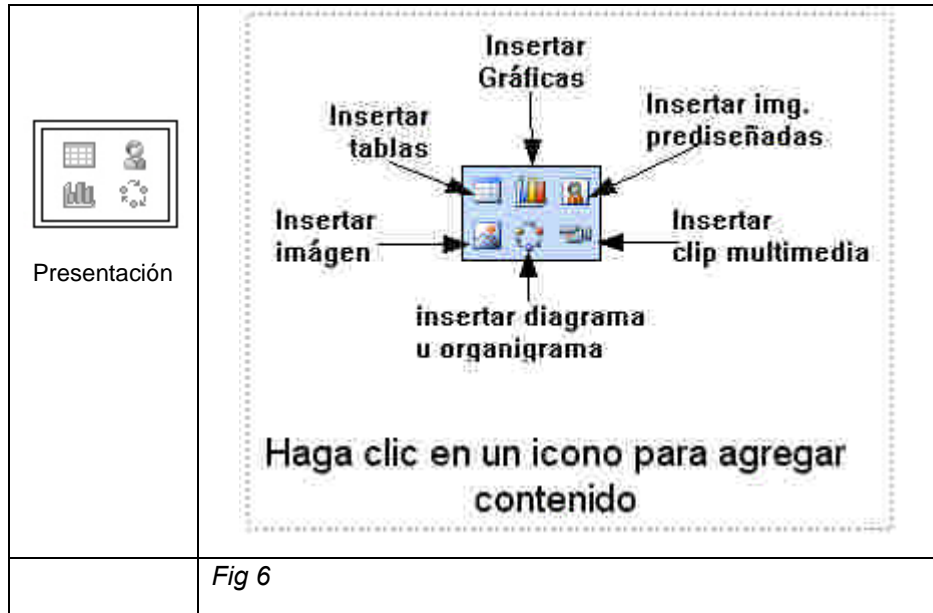
5.3 Creación del aspecto de una presentación.

Como lo vimos en el inciso anterior hay diferentes formas de abrir un archivo, para crear una presentación desde dónde cada uno elige sus fuentes tipográficas, tamaños, colores y fondos o una plantilla la cual tiene predeterminados todos los elementos antes mencionados de forma agradable, legible y armónico, ayudando a controlar la apariencia de nuestra presentación. Fig 5

La presentación que elaboremos puede ser un multimedia, dependiendo de los elementos que se le agreguen y del tipo de presentación que se elija al comenzar a trabajar. Como se puede observar en la Fig 6, la iconografía nos permite insertar los



elementos necesarios, basta con dar un clic sobre el elemento que se desea insertar, ya sea desde nuestros archivos o los que ya tiene como predefinidos *PowerPoint*.



PowerPoint tiene la capacidad de insertar **sonidos y música** que pueden utilizarse en tus presentaciones. Para esto es necesario ir a la *barra de menú / insertar / sonido de archivo*. Posteriormente buscar y seleccionar el archivo de sonido que se desee. Fig 7

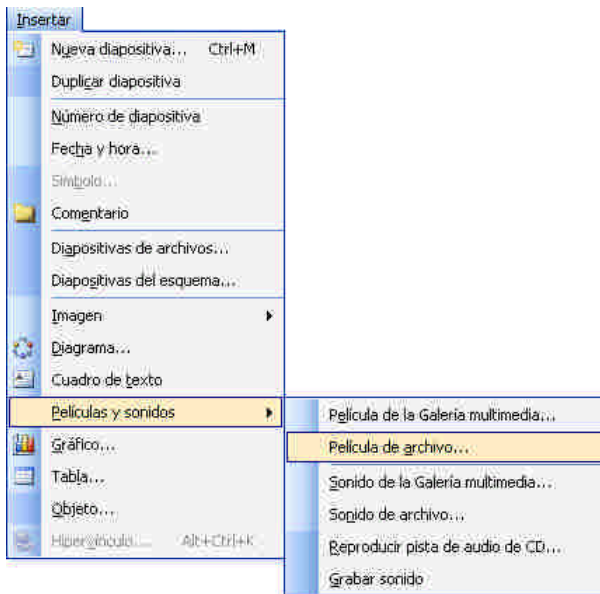


Fig 7


Clips de video. Para poder utilizar la galería de imágenes, hay que hacer clic *barra de menú / imagen / imágenes prediseñadas*.

Las combinaciones de colores son conjuntos de ocho tonos armónicos diseñados que pueden utilizarse como principales en una presentación con diapositivas (para texto, fondo, relleno, acentos, etcétera). Cada color de la combinación se aplica automáticamente a un elemento distinto de una diapositiva. Puede elegirse una combinación de colores para una diapositiva individual o para toda una presentación.

¿Cómo crear una presentación a partir de una plantilla?

Esta forma de generar presentaciones es muy cómoda y rápida, ya que sólo necesitamos ir agregado nuestros contenidos.



Desde el panel nueva presentación elige  **A partir de una plantilla de diseño** (a partir de una plantilla de diseño) se desplegará una lista de las plantillas existentes, sólo debes dar clic sobre el diseño que sea de tu agrado e instantáneamente se colocara en tu primer diapositiva, cada que insertes una diapositiva nueva a tu archivo conservara las características de la plantilla, obviamente habrá una pequeña diferencia en el acomodo y tamaño de la tipografía entre la principal y las interiores. *Fig 8*



Si el **panel de tareas** no está visible; lo podrás encontrar en el menú opción **Ver** y selecciona la opción **Panel de Tareas**.

¿Cómo crear una presentación a partir de un *asistente de autocontenido*?

Para crear una presentación a partir del *asistente de autocontenido* ² solo es necesario seleccionar esta opción y el programa te ira llevando de la mano para elaborar este proceso, es necesario ir llenando las celdas que te presentara a través de cinco pasos.

² Para elaborar un ejercicio interactivo de este tipo, te sugerimos que vayas a la siguiente dirección www... O a tu CD interactivo. Y sigas los pasos que ahí se te proponen.



1. El primero es “**iniciar**” (fig 5) al presionar siguiente aparece otra pantalla con más opciones por definir.
2. La segunda pantalla “**Tipo de presentación**”, nos proporciona diversas opciones sobre presentaciones estándar que podremos utilizar, las cuales se encuentran agrupadas en varios y amplios temas. Fig 9

En este ejemplo se ha seleccionado **Ventas y mercados / Plan de mercadotecnia**.

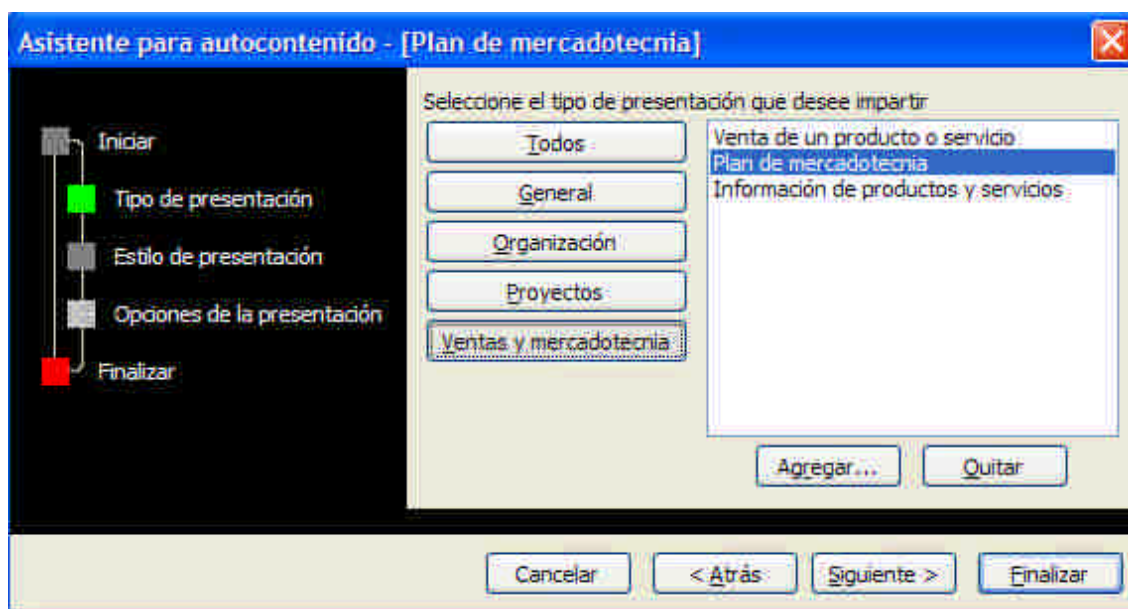


Fig 9

3. La siguiente ventana “**Estilo de presentación**” en ella se deben elegir el tipo de presentación que deseamos ya sea para Web, pantalla, transparencias o diapositivas de 35 mm. Fig 10

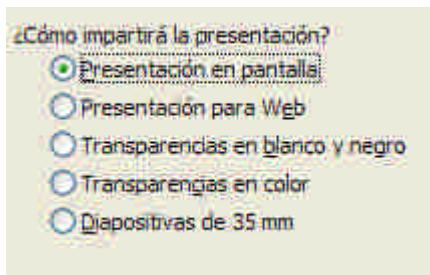


Fig 10

4. Para finalizar “**Opciones de presentación**” nos pide insertar el título de la presentación, además de elegir algunos otros elementos que desees que aparezcan en la diapositiva como: la fecha, número de diapositiva y pie de página. Fig 11

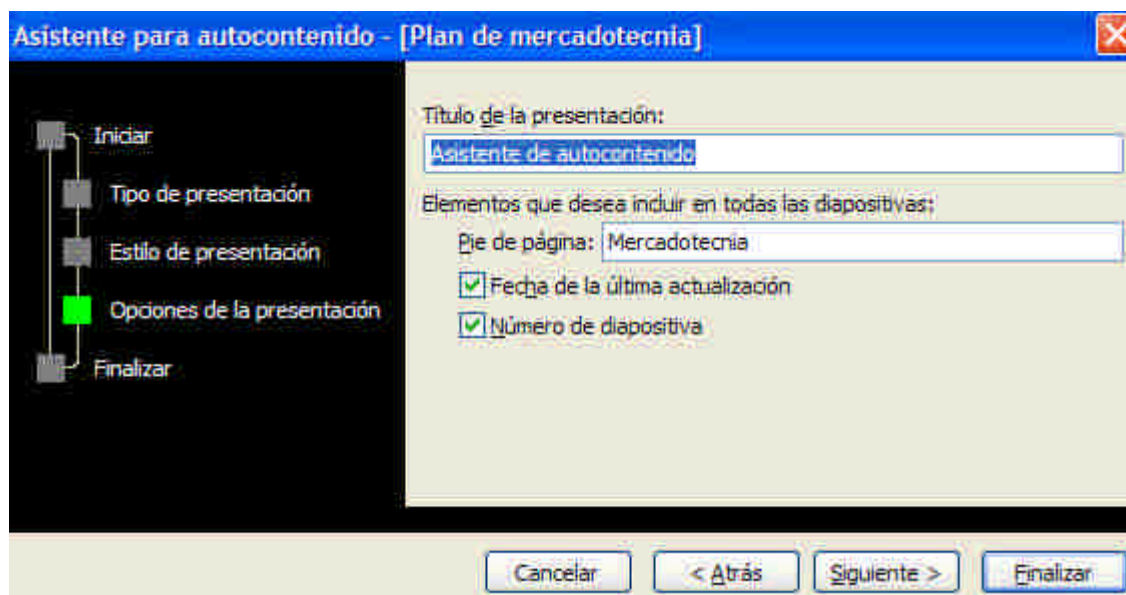


Fig 11

¡Listo! Ahora ya tienes una presentación generada por el **asistente de contenidos**, lista para que insertes la información necesaria en el orden que el programa te propone.

Si eres observador te darás cuenta que apareció del lado izquierdo una pestaña que dice “**esquema**” la cual te presenta las opciones propuestas dependiendo del tema



que ayas elegido. Las diapositivas te van llevando de la mano para darle un orden y lógica a tu contenido comenzando con el título, la introducción, temas a discutir, etc. Diapositivas en las cuales será necesario solamente insertes el texto que desees presentar o en su defecto borrar la diapositiva que no se vaya a utilizar. *Fig 12*

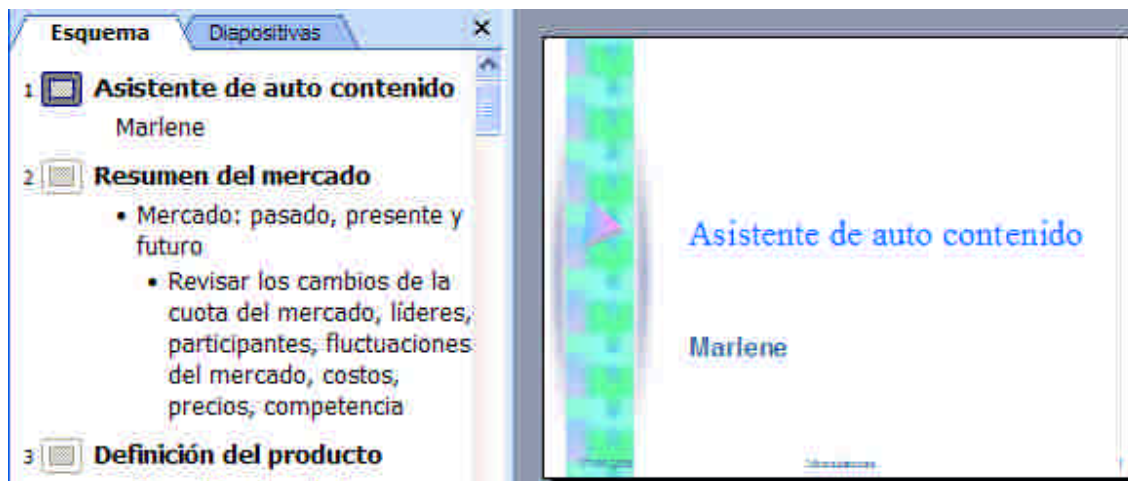


Fig 12

Las otras dos formas que existen para crear una presentación, por su facilidad, te sugerimos que las pruebes tú sólo o con la ayuda de las lecturas que se te han recopilado para esta unidad.

5.4 Patrón de diapositivas.

Las diapositivas o transparencias constituyen las páginas de una presentación. El patrón de diapositivas es un elemento de la plantilla de diseño³ este patrón está dedicado a almacenar información sobre la misma y controlar el formato en cuanto a

³ Plantilla de diseño: archivo que contiene los estilos de una presentación, incluido el tipo y el tamaño de las viñetas y fuentes; posiciones y tamaños de los marcadores de posición, diseño de fondo y combinaciones de colores de relleno y un patrón de diapositivas y el patrón de títulos opcional.



la colocación de los títulos (el estilo de fuente, tamaño y color), la ubicación y disposición de los gráficos que aparecerán en todas las diapositivas (logotipos o fondo), formas geométricas, imágenes y obviamente las combinaciones de colores en la cual interfiere el color de fondo, del texto, para formas geométricas o líneas y otros elementos.

Cualquier cambio realizado en el patrón de diapositivas se reflejará en todas las diapositivas. Si se quiere que la apariencia de una diapositiva individual sea diferente del patrón, puede modificarse sin tener que cambiar el patrón.

Para crear un patrón de diapositivas es necesario ir al menú **ver/patrón/ patrón de diapositivas**. Inmediatamente nos da una hoja en blanco a la cual podemos ponerle las características que deseemos como ejemplo puedes observar en la figura 13. Estas características las tomaran todas las diapositivas que se vayan generando a través del patrón.

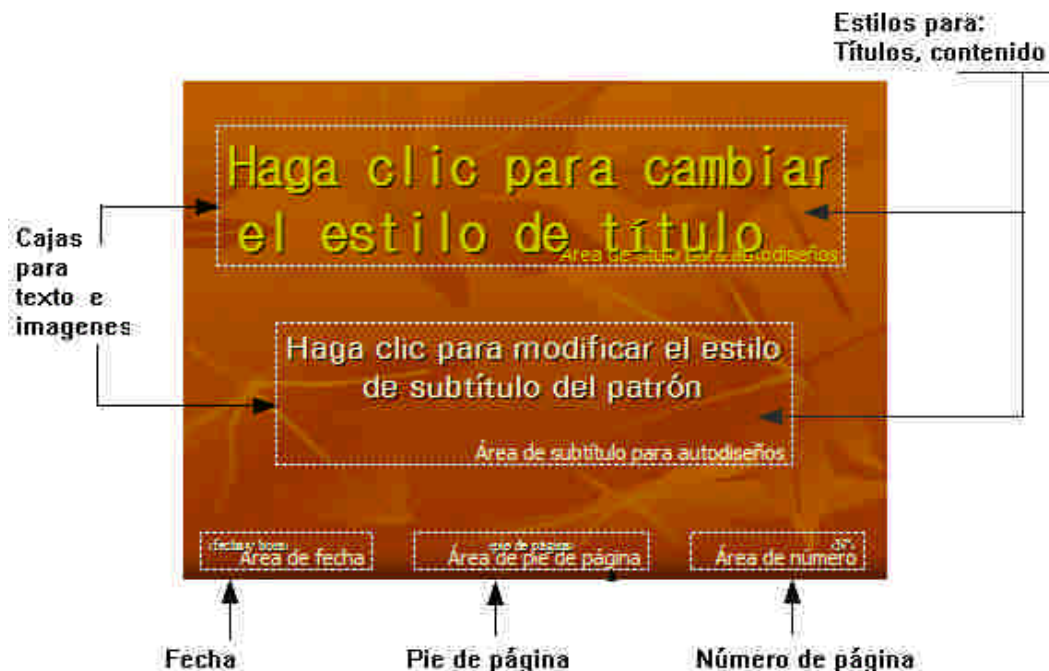


Fig 13



Un documento PowerPoint puede tener más de un patrón, los cuales puedes ir combinando con forme los necesites. Estos patrones se pueden modificar o borrar.

Fig 14

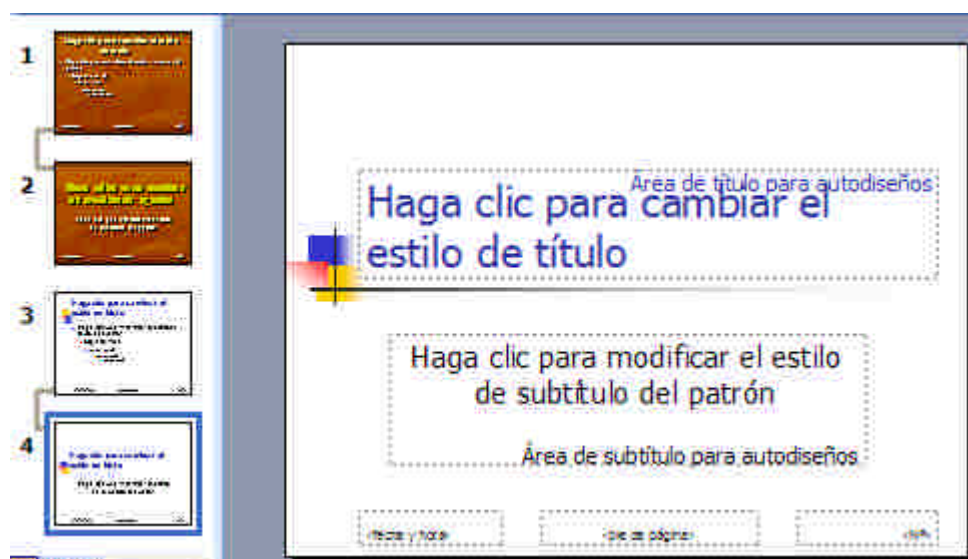


Fig 14

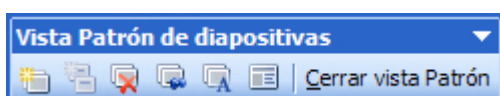


Fig15 Desde el momento que inicias el diseño de un patrón de diapositivas, aparecerá una ventana como la que se te muestra en la Fig 15 la cual te va ayudando a crear más patrones o a editarlos (cambiar nombre, borrar patrón y cerrar vista patrón).

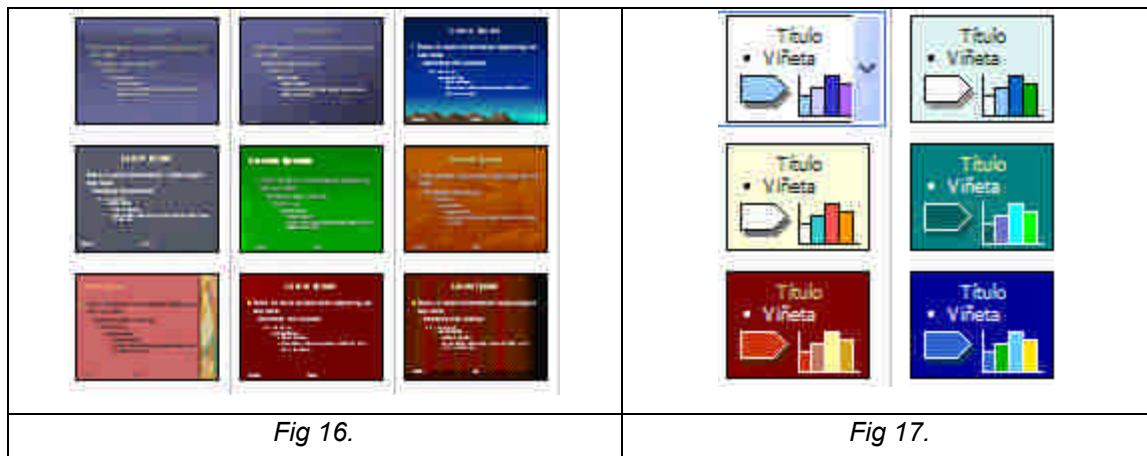
Una vez que ayas definido el o los patrones necesarios presiona **“Cerrar vista patrón”** esta opción te dará un archivo nuevo para que puedas comenzar a trabajar.

5.5 Plantillas.

PowerPoint incluye una amplia variedad de plantillas profesionalmente armonizando el fondo con la tipografía diseñadas para una buena presentación en pantalla como



ya te habíamos comentado anteriormente. Las plantillas pueden ser muy útiles, ellas contienen combinaciones de colores, patrones de título, diapositivas con formatos y fuentes personalizadas, elaboradas para conseguir una apariencia determinada. *Fig 16.* El programa también cuenta con plantillas de colores, las cuáles contienen 8 tonos armónicos distintos sólo basta con elegir la combinación deseada. *Fig 17.*



Cuando se aplica una plantilla de diseño a una presentación, esta se insertara automáticamente en todas las diapositivas que ya estén elaboradas y por supuesto cada diapositiva nueva tendrá la misma apariencia.

Pero no es necesario que te limites a las plantillas ya existentes recuerda que tu puedes generar tu propio patrón de diapositivas con los elementos y colores que desees integrarle.

5.6 Imágenes

Es cierto una imagen⁴ vale mas que mil palabras, y cuando se refiere a presentaciones la imagen es un herramienta poderosa, una ayuda excelente cuando se quiere decir un mensaje o idea, por muy abstracta que esta sea. Además de

⁴ Una imagen puede ser el detonador correcto para la total comprensión de la idea, o el entendimiento erróneo del mensaje.



proporcionarle a nuestra presentación algo más que texto, logra enriquecerla asegurando la atención de nuestro auditorio, combate el aburrimiento y refuerza el mensaje. Introduciendo imágenes en nuestra presentación será la mejor manera para lograr mejores diseños y llamativos enfoques, el énfasis de algún concepto o solución.

Existen dos tipos de imágenes en *PowerPoint*, las imágenes predeterminadas y las imágenes desde archivo.

Imágenes predeterminadas: son las imágenes que vienen dentro de la aplicación, es decir al momento de instalar nuestro programa nos pregunta si deseamos instalar imágenes de apoyo o predeterminadas después estas imágenes se almacenaran en nuestro disco duro y serán llamadas cuando el usuario decida ocuparlas, se puede tener mas de estas librerías integrando los clip arts a nuestras imágenes predeterminadas.

Este tipo de imagen es edítale dentro de *PowerPoint*, tanto en color como en brillo, elementos etc.

Imágenes desde archivo son las imágenes propias, ya sea tomadas por una cámara o descargadas del Internet, de algún catalogo etc. Es decir casi cualquier imagen digital solo condicionado a el formato de descripción de mapa de bits.

Los **formatos** se refiere a como nuestra imagen, es codificada para su visualización es decir en la manera en que fueron técnicamente preparadas para su descripción en la pantalla, este método de cómo fueron decodificados marcara la diferencia entre si se pueden importar dentro de nuestro proyecto o no. A continuación los formatos aceptados por *PowerPoint* y una pequeña descripción de los mismos.



Formatos de imágenes predeterminadas

.cil este formato se refiere a las imágenes prediseñadas por Windows se puede encontrar algunas cuando se instala el programa o bien se pueden descargar de la pagina de office, la cual proporciona una sección de apoyos donde encontraras una amplia galería por temas.

<http://office.microsoft.com/clipart/default.aspx?lc=es-mx>

El formato **.cil** es exclusivo de Office, la ventaja que posee este tipo de imagen en relación a los otros formatos es que tiene la capacidad de ser modificada, en cuanto al color, tamaño, brillo, y es posible modificar cada uno de los colores en grupos de gamas manipulándolos por tonos y relleno.

Formatos de imágenes desde archivo

JPEG- Joint Photographic Experts Group (JPEG), es te formato esta dado por un grupo de expertos en fotografía que se unieron para crear un estándar para imagen digital, que tuviese la compresión requerida por la época del Internet y calidad suficiente para verse clara y nítida. Este grupo es el creador de varios formatos como el del **dvd**, **mpeg4** y el formato de música más popular **mp3**.

El formato **jpeg** es altamente recomendado, algunas de sus cualidades es la compresión correcta para fotografías conservando una adecuada calidad y peso liviano. Algunas de las desventajas de este formato es que no tiene transparencia es decir, siempre nos mostrara un color de fondo solidó en el cual fue trazado el elemento o imagen.

PNG- Este formato fue creado por *Macromedia* para tener capacidades diferentes y propias de las imágenes jpeg y con la ventaja que este archivo si es transparente en su modalidad, **.PNG-24**. Este formato puede ser exportado desde la mayoría de



editores de imágenes como *Photoshop* o *Fireworks*. También tienen calidades de colores es decir pesos diferentes y un número de colores requerido.

BMP- Este formato de imágenes es creado por Windows contiene una compresión menor, es decir pesa menos pero su calidad es mayor que jpeg y no tiene transparencia. Es un mapa de bits bien definido y no compresado. Su desventaja podría ser el peso, ya que al contener mucha calidad el peso por naturaleza se eleva en gran medida.

GIF (formato de intercambio de gráficos) este formato fue creado exclusivamente para gráficos es decir no es bueno con fotografías, ni con degradados, pero su peso es muy bueno en gráficos y calidad optima, ya que esta descrito por colores ya sea 2, 4, 8, 32, 64, también tiene un formato con transparencia, el *gif89*.

PICT Y TIFF Son formatos creados para *Macintosh* que tienen una compresión liviana pero gran calidad. Estos formatos no son tan comunes para usuarios de *PC*.

Los antes mencionados fueron los formatos más generales e importantes que se pueden importar en nuestra presentación de *PowerPoint*.

Un valioso consejo.

No tomar a la ligera, de donde obtenemos estas imágenes, ya que generalmente pueden estar protegidas y estaríamos cometiendo un delito al utilizarlas. Con el desarrollo de Internet existen varias compañías productoras de bancos de imágenes, que ese dedican a venderlas, donde el cliente paga la imagen y puede hacer el uso de ella, ya sea temporal o definitivamente dependiendo del acuerdo que hayan tenido ambas partes. Aunque estas imágenes parecen ser “libres”, no lo son, el creador puede demandar si se ocupan sus imágenes sin consentimiento. No importando si



las ocupamos comercialmente o sin fines de lucro las imágenes están protegidas por leyes internacionales.

Nosotros también podremos proteger nuestras imágenes, por medio de copyrights en la oficina de derechos de autor, en algunas veces no es necesario, solo mostrando el proceso de creación se puede dictaminar quien hizo la imagen, para evitar la piratería.

Insertar imágenes en *PowerPoint*

La metodología para insertar imágenes en *PowerPoint* es desde el *menú, insertar imagen y escoger si es predeterminada o desde un archivo personal*. Fig. 18

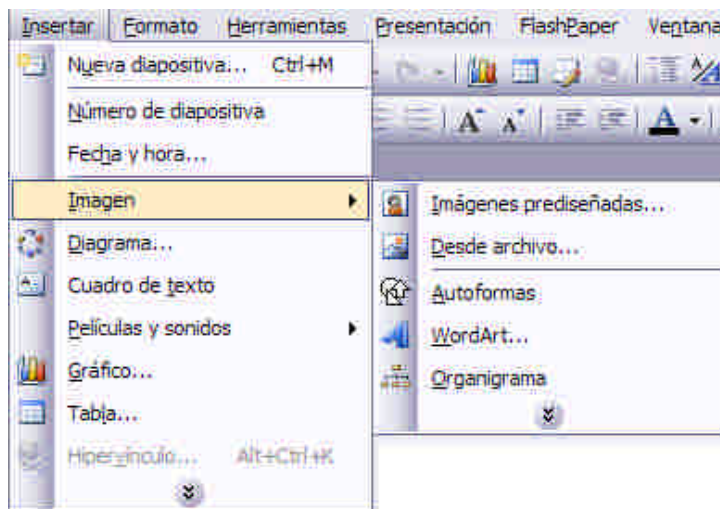


Figura 18

Si se requiere la **imagen prediseñadas** abrirá el siguiente cuadro Fig. 19 preguntándonos de dónde obtendremos la imagen, ya sea desde nuestra librería de imágenes, de la aplicación o de alguna librería externas como la librería Microsoft de Internet o algún banco de imágenes.

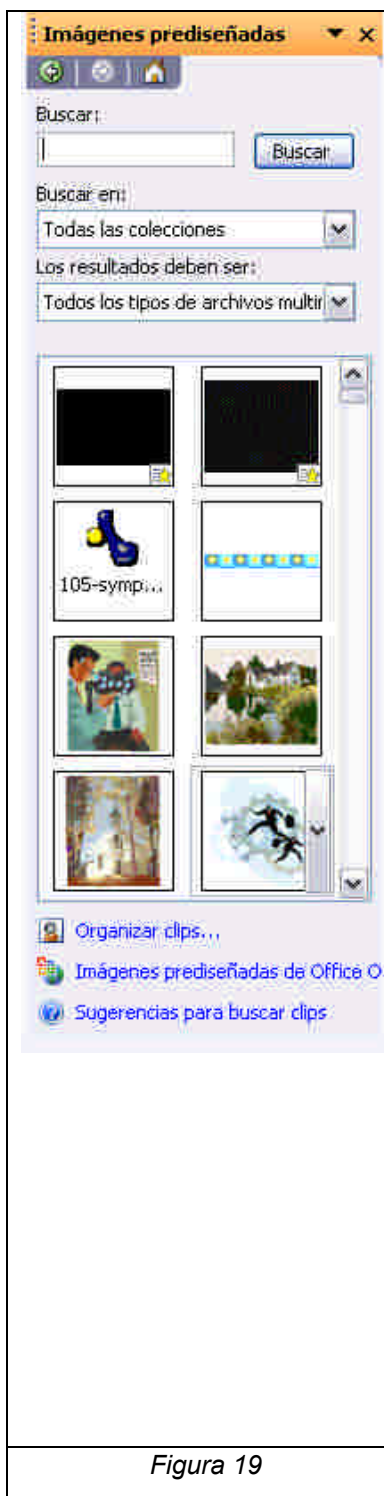


Figura 19

Dentro de esta ventana existe un inciso donde están todos los archivos multimedia como: video, imágenes personales y música sonidos etc. Esas cuestiones multimedia se verán mas adelante.

Lo primero que aparece es un campo para buscar los contenidos, puede buscar imágenes de *Windows*, sonidos, películas. Abajo cuenta con una sección que dice **organizar clips**, esto haría que en nuestro banco hubiese añadido todos los sonidos imágenes y películas de nuestra maquina compatibles con *PowerPoint*.

Cuenta con una pequeña ayuda de cómo insertar imágenes en la librería, como buscarlas, etc.

El paso final es una vez encontrada la imagen que deseemos simplemente la arrastramos al escenario y la añadirá a la diapositiva que este seleccionada en ese momento.

La imagen dentro del escenario presentara una serie de **nodos** o puntos con los cuales podremos modificarla: escalarla, rotarla, girarla, en fin modificarla completamente como se necesite.

En las **imágenes predeterminadas** existe un inciso donde se les puede cambiar el color a las mismas, solo basta con un doble clic a la imagen misma y sale un pantalla



que dice ***imagen/formato de imagen/volver a colorear***. Esta opción nos da la posibilidad de cambiarle los colores internos a la imagen como lo muestra la *Figura 20*, y de esta manera podremos armonizar más los tonos de la imagen a nuestro diseño de una forma más personal.

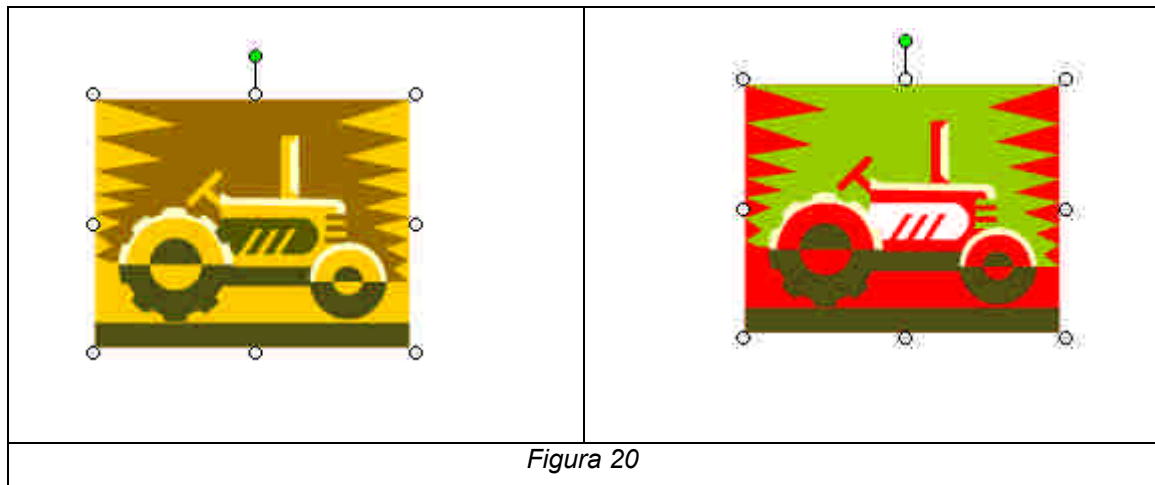


Figura 20

El
pro
gra
ma
con
tien
e
una
barr

a de herramientas *figura 21* la cual también nos permite hacerle modificaciones a la imagen, cambiando el brillo, el contraste convertirla en tonos de grises, cortar, rotar y muchas otras.





La siguiente barra de herramientas *Figura 21* es muy útil para la edición de las imágenes, basta con seleccionar el dibujo o fotografía y está aparecerá.

A continuación se explicaran los iconos para que conozcas a fondo la forma de trabajar de cada una de ellas.










Figura 21







	<p>El primer icono tiene como función, la de insertar una imagen o fotografía ubicada en cualquier parte de nuestra computadora.</p>
	<p>Cambia el aspecto de la imagen seleccionada, si se selecciona la opción escala de grises la imagen se convertirá en blanco y negro.</p>
	<p>Más contraste Aumenta el alto contraste a la imagen en forma gradual, hasta el grado de llegar a desaparecer ciertos tonos de la imagen.</p> <p>Menos Contraste Disminuye el alto contraste, también en forma gradual dándole al usuario la posibilidad de decidir hasta que nivel hace la disminución del contraste. Si se abusa de esta herramienta la imagen se convertirá en una mancha de color gris. <i>Figura 22</i></p> <div data-bbox="604 1102 1068 1312" data-label="Image"> </div> <p style="text-align: right;"><i>Figura 22</i></p>
	<p>Los siguientes iconos sirven para detonar la acción del brillo, el icono Más brillo aumenta la luz hasta llegar a una mancha blanca o una imagen apenas imperceptible; por el contrario el segundo icono Menos brillo quita el brillo de una imagen hasta llegar a convertirse en una mancha negra, <i>Figura 23</i> como se puede observar el siguiente ejemplo.</p>



	 <p>Más brillo Menos brillo <i>Figura 23</i></p>
	<p>El siguiente icono sirve para recortar la imagen, es necesario seleccionarla y presionar la herramienta de recorte, a esta le parecerán unos nodos, es decir puntos en los extremos para tomar solo el fragmento de la imagen que necesitamos. Podemos jalar estos nodos ya sea de izquierda o derecha de arriba o abajo y enter para que lo aplique. <i>Figura 24</i></p>  <p><i>Figura 24</i></p>
	<p>La siguiente función es la de rotar, al momento de hacer clic sobre la imagen está se rotara 90 grados cada vez que se le aplique.</p>
	<p>Sirve para enmarcar nuestra imagen, un rectángulo rodeara nuestra imagen dependiendo del tipo de línea elegido. <i>Figura 25</i></p>  <p><i>Figura 25</i></p>
	<p>Una opción importante es la de <i>comprimir imágenes</i> está nos es muy útil para el resultado final de nuestra proyección, es decir este optimizador de imagen reduce el peso de las mismas para tener mejor desempeño en la presentación y es</p>



	mejor para su visualización en Internet. Tiene parámetros para optimizar para Internet o para impresos.
	Con esta herramienta se pueden cambiar los tonos de las imágenes como lo vimos en la <i>Figura 20</i> , siempre y cuando correspondan a la galería de imágenes del mismo programa.
	Abre una ventana desde la cual podemos manipular todas las opciones que hasta ahora hemos visto, en esta barra de herramientas.
	<p>Esta opción ayuda a sustraer un color determinado y convertirlo en transparente, <i>Figura 26</i> siempre y cuando la imagen no pertenezca al <i>clip art</i>, sino que sea una imagen de mapas de bits y sólo tiene la capacidad de extraer uno de los tonos.</p> <div data-bbox="634 1108 1024 1276" data-label="Image"> </div> <p style="text-align: right;"><i>Figura 26</i></p>
	<i>Restablecer imagen</i> es la última de las herramientas y su función es devolverle a la imagen su estado original, desde el tono del color hasta el tamaño, quitándole todos los cambios que se le hallan echo.



5.7 Formatos de texto

Si bien la imagen es importante para una presentación electrónica, el texto es fundamental, hay que tener en cuenta, que una presentación no debe manejarse como un tratado donde las palabras van por millones, debemos ser mas precisos en la elección de la cantidad y calidad de la información. Un error común en el texto es la elección de la fuente tipográfica y el tamaño adecuado, estos dos aspectos son muy importantes debido a que no importando el lugar o la distancia donde se hallé nuestro receptor pueda entender claramente el mensaje.

Aspectos necesarios que hay que tomar en cuenta a la hora de elegir la tipografía es que sea legible, que sea formal o informal dependiendo del tipo de platica y el usuario destinado. Para la lectura en pantalla se recomiendan las llamadas fuentes de palo seco; son aquellas que no tienen remates y que no están muy elaboradas, por ejemplo: Arial, Helvetica, Tahoma, SansSerif, ten por seguro que con estás se podrá leer muy bien el mensaje.

El color debe ser contrastante en cuanto al fondo de la diapositiva, por ejemplo si se usa un color de fondo oscuro el texto deberá ser claro y a la inversa si el fondo es claro la letra deberá ser oscura.

Una vez que conoces los criterios para la elección de la fuente tipográfica optima, veremos como insertar un capo de texto.

Ve al menú **Insertar / cuadro de texto** (de la barra de menú). Notaras que el cursor cambia a una cruz invertida la cual es necesario posicionar en el lugar deseado y con un clic sostenido y arrastrando el Mouse creara una caja destinada al texto. Como la

Figura 27

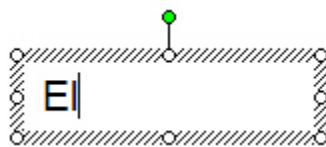


Figura 27



Para la edición de la tipografía⁵, tamaño, color, fuente, alineación, etc. Nos ayuda la barra de formato *Figura 28*

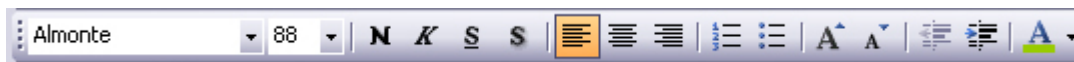



Figura 28

La primer celda nos especifica el tipo de letra, la siguiente su tamaño (generalmente esta dado en números pares y múltiplos de 4), los números están dados hasta el tamaño 96, pero en caso de requerir una fuente más grande se puede dar doble clic sobre el número y escribir el tamaño deseado aumentándolo hasta 999 puntos.

La siguiente división esta dada por los estilos de la tipografía el primer estilo es **las negritas** representado con una **N**, *ITALICO* representado por un *K*, con una letra S el subrayado⁶. Estas opciones son estilos de tipografía, para resaltar alguna palabra en especial o recalcar una oración y/o párrafo.

Posteriormente puedes observar dos letras **A** una más grande que la otra, estos iconos sirven para aumentar o disminuir un punto a la tipografía, junto a ellas esta la opción estan los iconos de aumentar o reducir sangría.

Y por último la opción  es el comando para darle color a nuestra tipografía automáticamente contiene un color negro, al presionar la flechita negra nos mostrará otras opciones y algunos colores seleccionados anteriormente por nosotros y la opción de “Más colores...” las cuales nos permitirá escoger un tono de una gama de 255 colores de la paleta Web⁷ *Figura 29*. Existe también el **Modo Personalizado** *Figura*

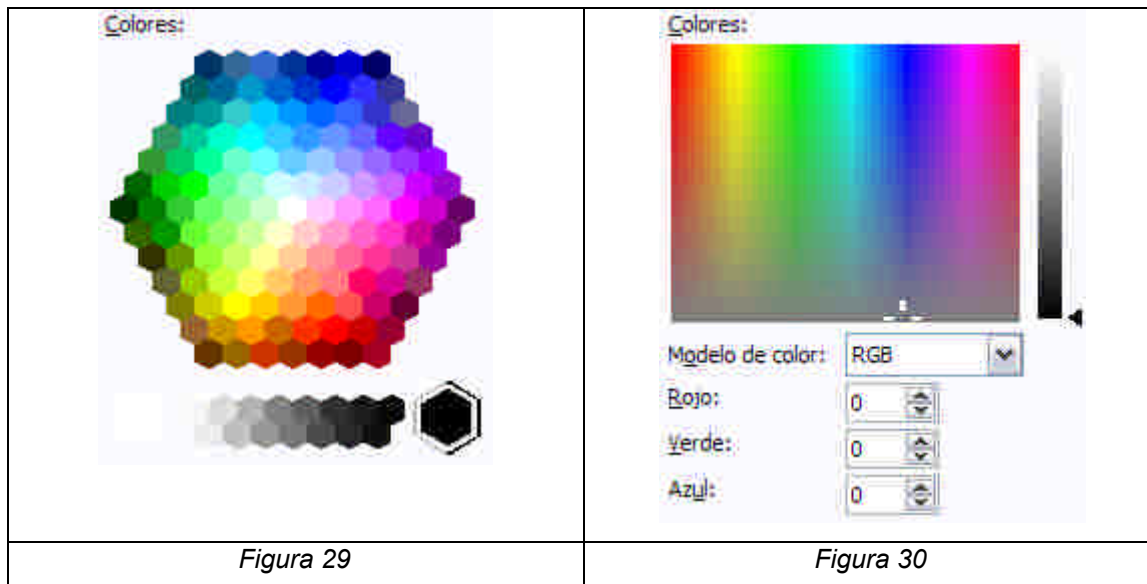
⁵ En caso de requerir una fuente que no existe en el sistema, será necesario instalarla desde el panel de control.

⁶ En esta época no es muy recomendable usar los subrayados ya que pueden confundirse con una Hiperliga dentro de la presentación.

⁷ Colores seguros para el Internet, son colores que no cambian su apariencia independientemente de la plataforma en que se vea (PC, MAC, Linux, etc.)



30 desde donde podremos seleccionar por porcentaje el color deseado, manipulando directamente los valores de RGB (RED, GREEN, BLACK) con la combinación de estas tres gamas podemos crear cualquier tono que deseemos.



Para seguir estilizando nuestro texto tenemos una opción más espectacular y de gran impacto, que es la opción de **Word Art**, esta opción tiene estilos predeterminados de texto con fugas, contornos y perspectivas a tan solo un clic *Figura 31*. Es una opción fácil de ocupar se selecciona el estilo y se pone el mensaje tipográfico que necesitamos esto hará que nuestro texto adquiera un estilo, puede incorporar también las características especiales para los textos, así como modificarle su dirección y sus colores para lograr el efecto deseado.

Pero cuidado solo se recomienda este tipo de efectos en títulos o mensajes importantes que se requiera resaltar, no es recomendado en párrafos podría ser caótico por la complejidad de la lectura y la organización del mensaje.



Figura 31

5.8 Impresión de Presentaciones.

No es muy común que se impriman las presentaciones, generalmente la impresión es para tener una especie de guión escrito con notas y consejos para el expositor. La manera de mandar a impresiones es la siguiente. Desde menú *Archivo / imprimir* despliega la siguiente ventana *Figura 32* que básicamente contiene las características generales de impresión de cualquier otro programa. Como el seleccionar la impresora (en caso de tener varias), la calidad el color (media, alta o baja), el número de paginas e impresiones, etc.

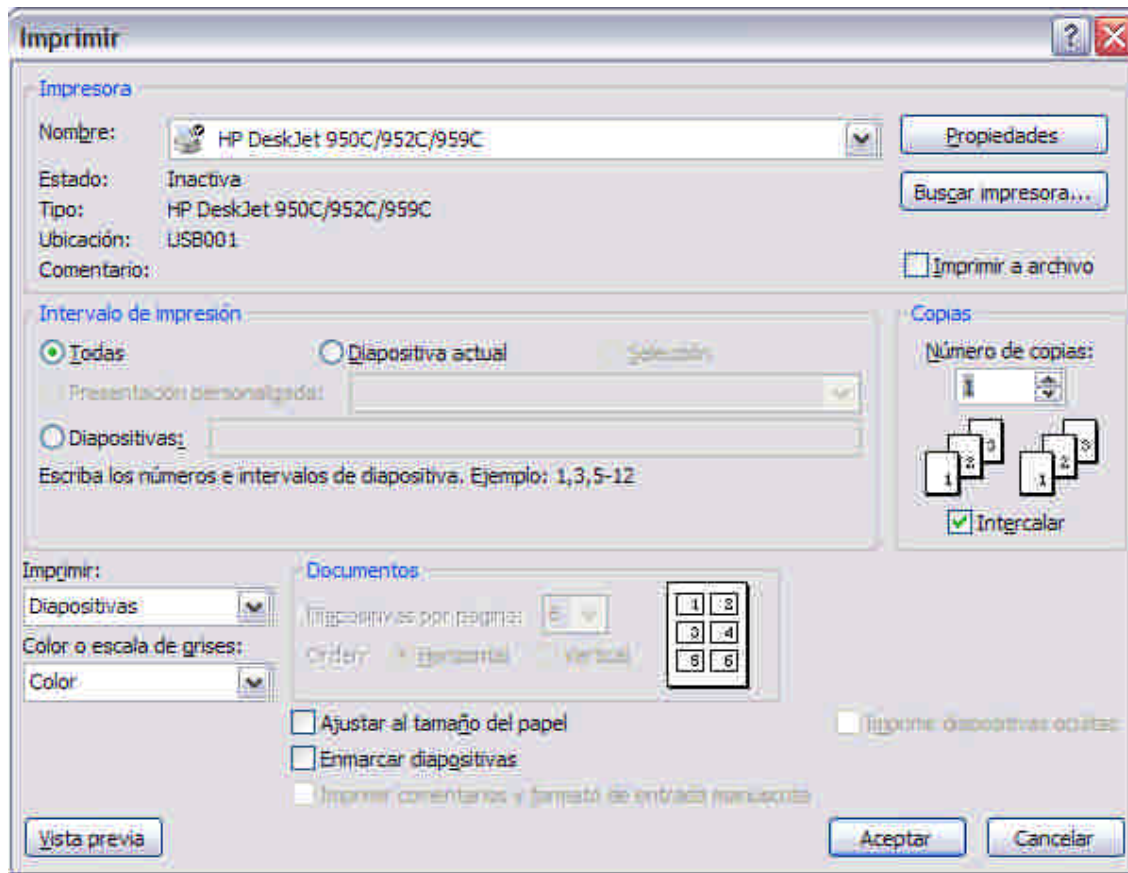


Figura 32

Aunque existe una parte importante y específica de PowerPoint *Figura 33* donde en la ventana desplegable de la opción **imprimir** nos da las siguientes opciones:

Diapositivas: imprimirá una diapositiva por hoja, útil para crear acetatos.

Documentos: imprimirá miniaturas de diapositivas, ya sea (dependiendo de la opción que elijas) de 1,2,3,4,6 y 9 diapositivas por hoja. La de tres nos imprimirá algunas líneas delante de la diapositiva para tomar notas. Como lo puedes ver en la *figura 33*

Sólo desglosamos de manera amplia estas dos opciones aunque existen cuatro debido a que son las más utilizadas.



La sección de **color** permite mandar la impresión en escala de grises o en blanco y negro.

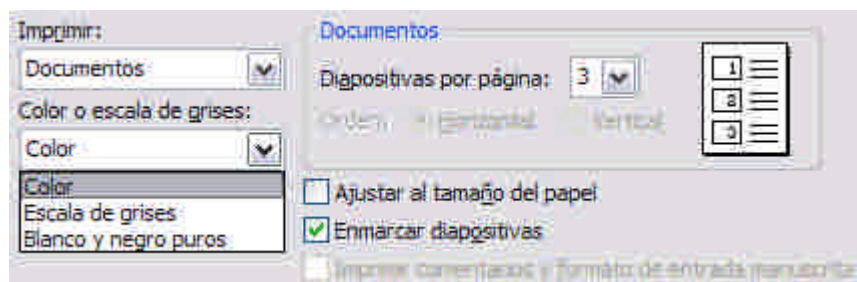


Figura 33

5.9 Ecuaciones, tablas y gráficas en una presentación

Las **ecuaciones** en PowerPoint son insertadas como un objeto exterior a nuestra presentación es decir, PowerPoint llama aplicaciones exteriores de la familia Microsoft como auxiliares en su desempeño. La manera de insertar un objeto que genera ecuaciones es la siguiente. Menú *insertar / objeto / Microsoft editor de ecuaciones 3.0* Figura 34

Esta opción desplegará una pantalla emergente desde dónde se podrán generar las diferentes ecuaciones, con los símbolos necesarios, además de los cálculos y al momento de cerrar este editor aparecerá la ecuación en la diapositiva en la cual nos encontremos trabajando.

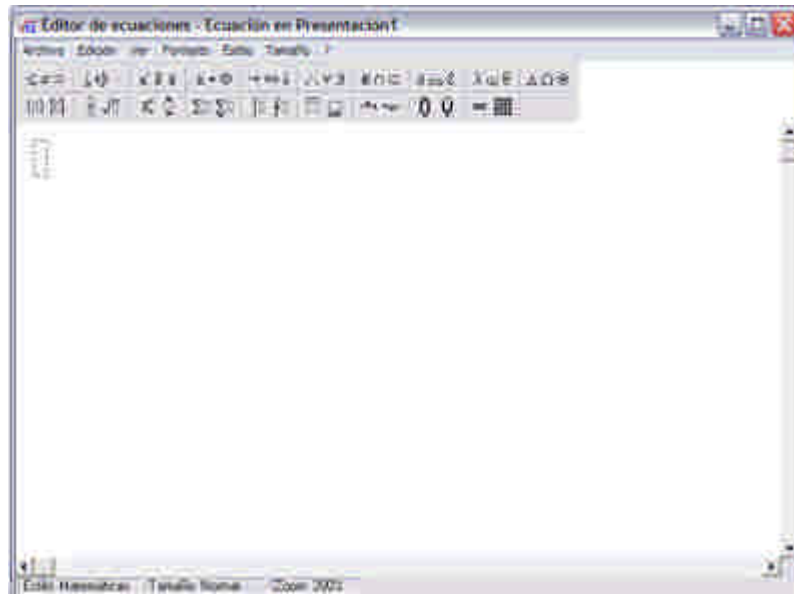


Figura 34

Tablas

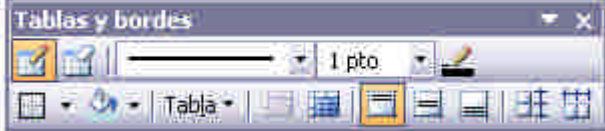
Las tablas son un elemento fundamental para organizar nuestra información en sectores de nuestra diapositiva, además de ayudar a jerarquizar los contenidos; la forma de crear una tabla es en el menú *insertar / tabla*, y nos muestra una ventana *Figura 35* en la que escribimos el número de columnas y de filas que necesitamos, se insertará una tabla en la diapositiva en la que estemos trabajando. Aun ya creada la tabla se puede agregar o eliminar celdas, filas o columnas, cuando lo deseemos, con dar clic derecho seleccionando el área deseada para sumar o substraer elemento⁸.



Figura 35

⁸ Es igual a la forma de trabajar tablas en Word.



 <p>Figura 36</p>	<p>Cuando la tabla esta en nuestra diapositiva nos aparece una ventana nueva <i>Figura 36</i> con varias opciones para la edición de la misma.</p>
--	--

A continuación de manera general se explicarán los iconos que contiene esta ventana.

- En la parte superior derecha *un lápiz*, con el cual podemos trazar nuevas celdas, filas y celdas cruzadas.
- El icono con tabla y goma es para borrar celdas, filas y columnas
- El siguiente campo se refiere a contorno de la tabla y el tipo de línea que trazara el lápiz color y grosor que tendrán las futuros trazos
- En la parte inferior encontramos de derecha a izquierda una herramienta la cual sirve para elegir las líneas que deseamos se impriman. Estas se verán de color negro y las que no se imprimirán serán de color gris.
- La cubeta nos sirve para dar color al fondo de la tabla o celda, teniendo en cuenta que cada celda puede ser coloreada de un color independiente o por un degradado (horizontal, vertical o radial). También se le puede rellenar con una textura o con alguna imagen o trama *Figura 37*. Todo esto desde la opción **efectos de relleno** en la sección de color.



Figura 37



Gráficas en una presentación

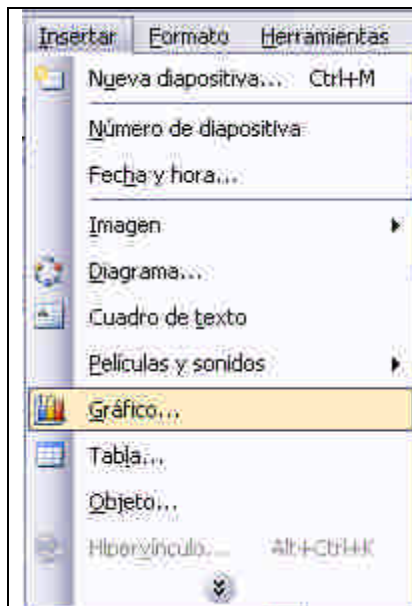


Figura 38

Una grafica se puede considerar como una manera visual de entender los números. Existen dos formas de insertar un grafico: desde el menú *insertar/grafico* Figura 38. Cuando lo seleccionemos insertara la aplicación un grafico genérico, que es el de barras planas. Cuando este aparece nos presenta 3 opciones y sus parámetros de manera genérica, es posible modificar estas características en cualquier momento.

Estas modificaciones de parámetros y nombres serán posibles en la hoja de datos ahí podremos agregar cualquier parámetro o cambiar el numero de cada inciso y renombrarlos acorde a como el usuario lo requiera. En el eje de los números de 1 al N tendremos las opciones de los nombre de cada uno esta dada por las

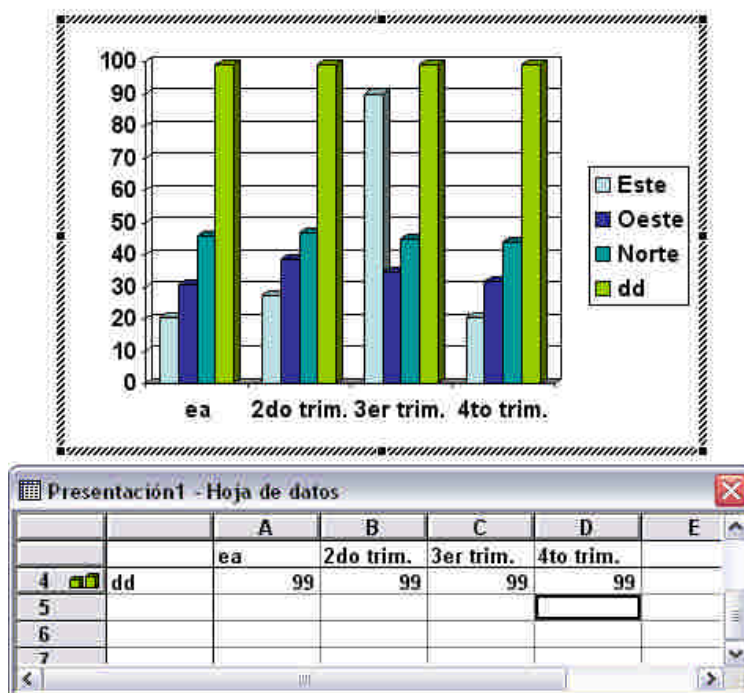


Figura 39



celdas numéricas en la primera columna, el nombre que tecleemos será el nombre de la variable, después en la columnas A;B;C;D;E hasta N encontraremos	
los parámetros de cada uno de las variables dependiendo de estas variables será el numero asignado en x de los valores es decir si hay variables de una unidad será dada por consideraciones de altura de unidades pero si las variables alcanzan millones este numero signado será visualizado en millones, En lo que refiere a la primera fila encontraremos los nombres asignados a cada periodo en Y, <i>Figura 39</i> . Este ejemplo fue solo llevado a la consideración que tenemos mas visualizaciones para adecuar cada una de ellas a las intenciones numéricas de nuestra presentación. Podremos cambiar el tipo de presentación para adecuar cualquier diseño ya sea a barras, pastel, puntos, cilindros 3d etc.	

Solamente seleccionando nuestro grafico, y dar un clic derecho y tipo de grafico ahí nos proporcionara una gama entera de diferentes gráficos *Figura 40* y opciones para modificar sus colores y apariencia, existe una opción de personalizados, ahí encontraras diseños que se lleven acorde a lo que necesita visualizar ya sea, avances, porcentajes, etc. Estadísticas modas, puntos de mayor alcance. En fin todo lo que se contenga en la hoja de datos pero resaltar el punto numérico que se desee.

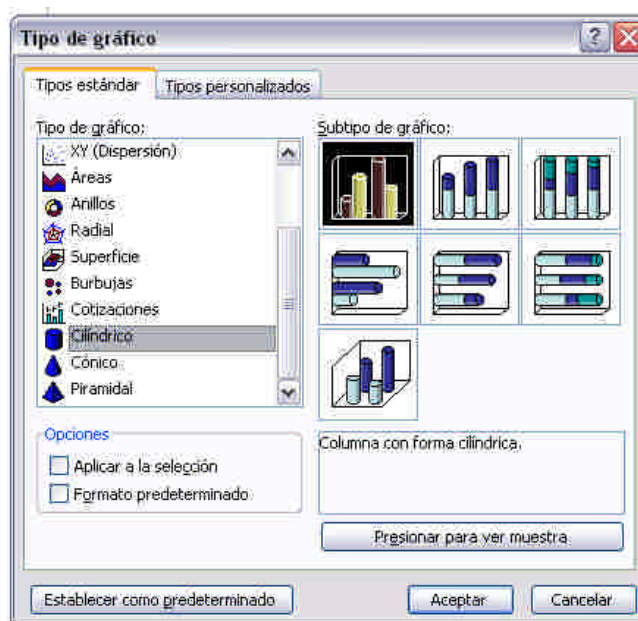


Figura 40

5.10 Presentaciones electrónicas

Una vez que la presentación este terminada será necesario exportarla de manera que solo un proyector que podamos ejecutar y controlar a nuestra disposición. Este proyector tiene la peculiaridad que no se puede editar, nadie puede tocar los elementos contenidos en el, de esta manera las diapositivas se encuentran protegidas. Para exportar este "formato" tendremos que ir al menú *archivo/guardar como/presentación de diapositivas en PowerPoint*, esto nos permitirá guardar el archivo con una extensión **P.D.**, la cual contiene con todos los elementos comprimidos y optimizados para una mejor ejecución. *Figura 41*

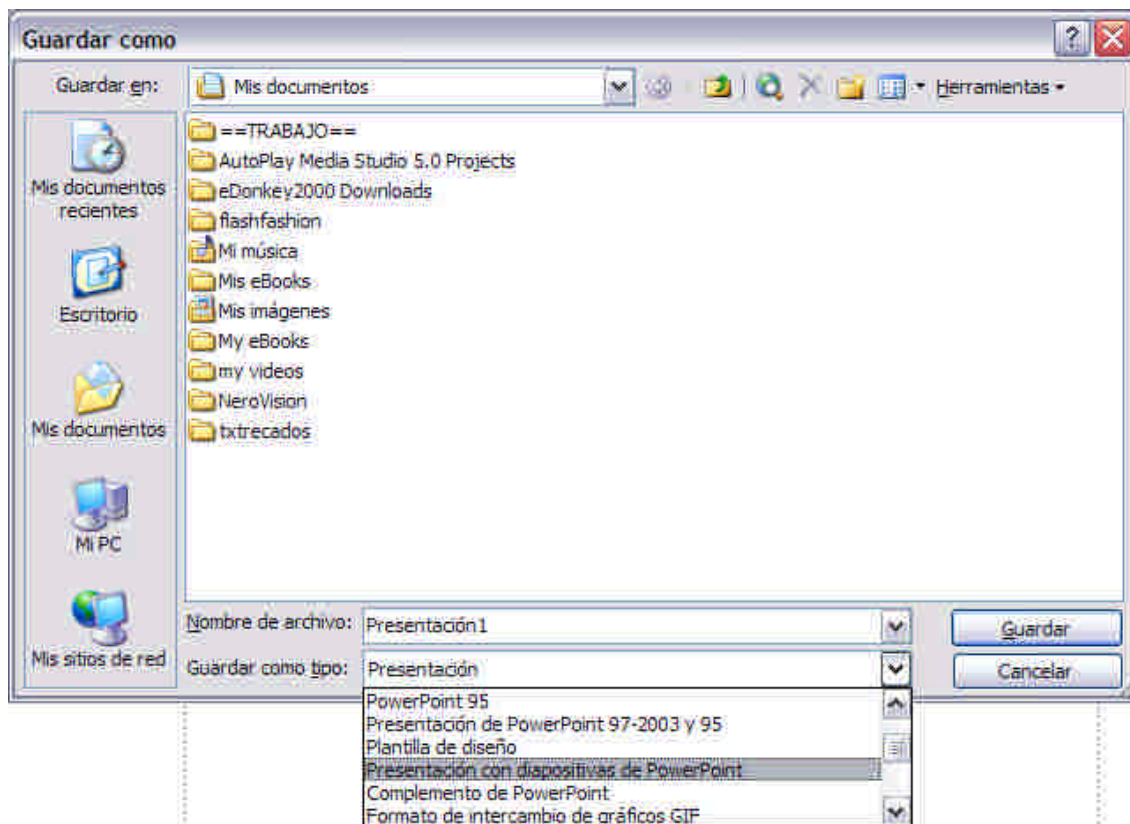


Figura 41

Existen otros formatos requeridos para exportar nuestro trabajo pero el que nunca debemos de olvidar ese el formato que nos permite editar nuestros elementos textos, imágenes y seguir integrando diapositivas o conformando diferentes acomodados y diseños en otras palabras el editable, para guardar este archivo es necesario ir al *menú archivo/ guardar como* y se elige la opción de presentación de *PowerPoint*, el archivo se guardara con la extensión **PPT**.

5.10.1 Ejecución y control de una presentación

Al momento de exportar nuestro proyecto, tendremos un proyector con la presentación terminada mostrándose a pantalla completa, lo que nos dará la opción de manipularla de alguna forma, subrayar, cerrar etc. Esta opción se ubica en la parte inferior izquierda de nuestra proyección *Figura 42*.



Figura 42

La primera opción es claramente la indicación para pasar a la diapositiva anterior.

La segunda opción tiene que ver con marcadores de algún elemento teniendo como cursor la flecha por default (cuando habrá la aplicación), pero al momento de cambiar a bolígrafo, rotulador o marcador tendremos la posibilidad de resaltar cualquier elemento en las diapositivas subrayar cualquier anotación o selección a la que nos referimos verbalmente para acentuar el punto, o enumerarlo, personalizarlo con el trazo. Este trazo se hace a mano alzada dirigiendo el *Mouse*, Podemos seleccionar el color de tinta, un borrador para quitar algún elemento que hayamos marcado equivocadamente y una opción de visualización de este menú en opciones de flecha.

Figura 43

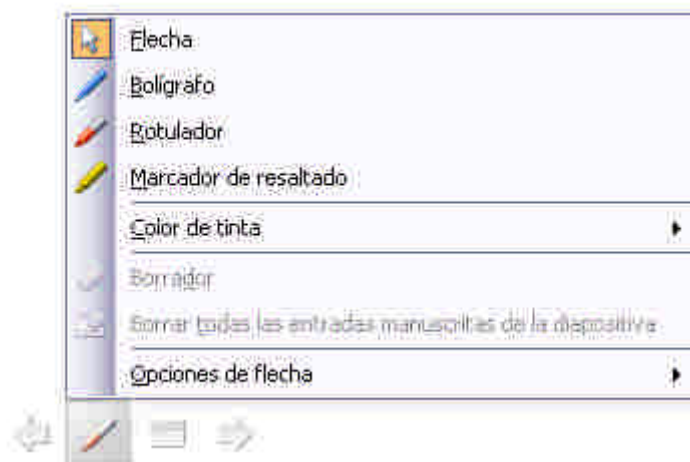



Figura 43



 <p><i>Figura 44</i></p>	<p>En el tercer icono, nos permite navegar entre las diapositivas del proyecto, ya sea por número, por anterior o siguiente. También cuenta con opciones de reproducción como pausa, cerrar la presentación, poner una pantalla de descanso blanca o negra que se restablecerá con un clic.</p> <p><i>Figura 44</i></p>
---	---

Para terminar concluiremos que lo más importante de una presentación no es la tecnología que se ocupa ni lo espectacular del mensaje si no, tener los puntos claros y dejarlos en la memoria de nuestro espectador de manera que el mensaje quede claro y entendido de manera como fue planeado.



ANEXO 1

Multimedios

nuestra presentación tiene el potencial de incorporar tanto archivos de audio, que sirvan como atmósfera o recalquen ciertas acciones o cambio de diapositiva. Y pueden reproducir alguna entrevista o palabras exactas directamente de los noticieros o la radio. La manera de insertarlos es desde el comando *insertar/películas y sonido* y ahí insertar sonido desde archivo *Figura 45*, al momento de insertarlo nos preguntara si deseamos que se escuche cuando pase la diapositiva o hasta darle clic en un icono con la bocina.

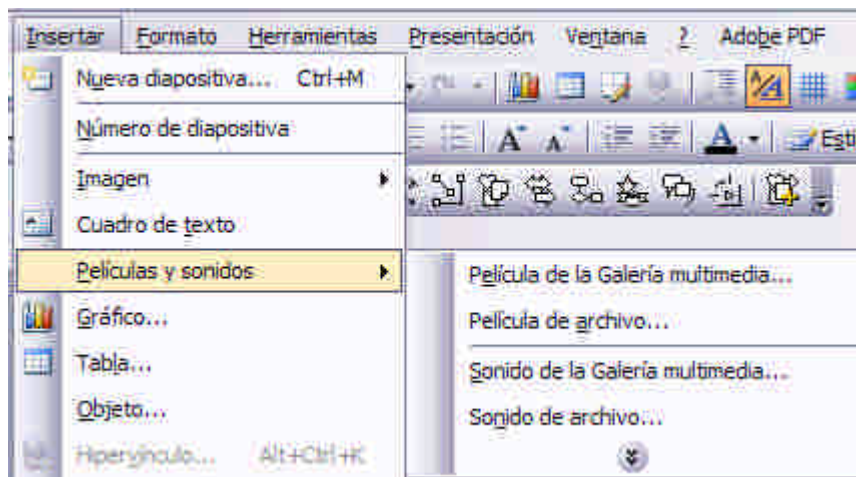


Figura 45

Lo mismo sucede con las películas de video aunque con sus limitaciones de proyección ya que los videos necesitan un reproductor y una decodificación adecuada para la visualización en diferentes usuarios. Los archivos de película son recomendados ampliamente, los archivos que manejan los decodificadores de Windows como el formato, *wmv* Windows media video, *avi*. Para asegurar que esto archivos se visualizaran en nuestras diapositivas debemos de asegurar que los archivos de video se encuentran en la misma ruta, en la que fueron insertados.