





# Informática Básica para Todos



Iniciando con la tecnología

**Jorge Lira Camargo**  
**Luis G. Lira Camargo**

**Autores:**

**Jorge Lira Camargo**

**Luis G. Lira Camargo**

**Editado por:**

**Jorge Lira Camargo**

**Av. Paseo de la República 4095 – Lima**

**[jlira@sesu.net.pe](mailto:jlira@sesu.net.pe)**

**Diseño de portada:**

**[autoreseditores.com](http://autoreseditores.com)**

**Primera edición digital, febrero 2021**

**ISBN: 978-612-00-5989-0**

**Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2021-01451**

**Disponible en [autoreseditores.com](http://autoreseditores.com)**



## *Dedicatoria*

A nuestros padres por los ejemplos de perseverancia y constancia que los caracteriza y que nos han infundado siempre. A *nuestros hijos Alexander y Briana que nos motivan cada día a lograr nuestras metas.*

*Jorge Lira Camargo*  
*Luis G. Lira Camargo*

# Sobre los autores

Jorge Lira es Ingeniero de Sistemas de la universidad Nacional Hermilio Valdizan con estudios de doctorado en la especialidad de ingeniería de sistemas, enfocado en la transformación digital de las organizaciones y en la docencia universitaria.

Luis Lira es Ingeniero de Sistemas e Informático de la universidad de Huánuco con más de 15 años en docencia universitaria.

# ÍNDICE

Capítulo 1.....	10
Introducción .....	10
Componentes que conforma el Hardware .....	11
Componentes que conforma el Software .....	11
Capítulo 2.....	12
Copia de respaldo.....	12
Areca Backup .....	13
Cobian Backup .....	15
Mendeley.....	16
One Drive, Dropbox, Box, Google Drive y Icloud.....	16
Capítulo 3.....	18
Herramientas básicas .....	18
Microsoft Word .....	18
Inicio de Word .....	19
Microsoft Excel .....	20
Microsoft PowerPoint.....	23
Aula virtual.....	24
Capítulo 4.....	26
Formularios Digitales.....	26
¿Qué es un formulario digital? .....	27
¿Cómo los formularios digitales pueden beneficiar a tu negocio? .....	28
Aplicaciones para crear formularios online.....	29
Capítulo 5.....	32
Antivirus y Malware.....	32



Malware .....	33
Tipos de Malware .....	34
Virus.....	43
Antivirus .....	45
¿Cómo se elimina un virus?.....	48
Precauciones para evitar una infección .....	48
Antivirus Online.....	50
Las reglas del Firewall.....	55
Capítulo 6 .....	58
Documentos HTML5.....	58
¿Qué es HTML5? .....	59
¿Por qué es importante HTML5? .....	61
las nuevas etiquetas de HTML5.....	61
Las etiquetas nuevas importantes de HTML5 .....	64
Las nuevas expectativas de HTML6.....	65
Capítulo 7 .....	67
CSS y modelos de caja .....	67
CSS y HTML.....	68
Estilos .....	69
Estilos embebidos .....	71
Archivos externos.....	72
Referenciando con cualquier atributo .....	76
Aplicando CSS a nuestra plantilla .....	78
Modelo de caja tradicional.....	78
Creando la caja principal .....	80

# Capítulo 1

## Introducción

La informática es la disciplina tecnológica más importante de la actualidad. Los dispositivos tecnológicos como computadores o smartphones están compuestos por el conjunto de componentes físicos de los que está hecho el equipo, y el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo. El hardware es la parte que puedes ver y tocar de los dispositivos. Es decir, todos los componentes de su estructura física como pantallas y teclados. El Software son los programas informáticos que hacen posible la ejecución de tareas específicas dentro de un computador. Por ejemplo, los sistemas operativos, aplicaciones, navegadores web, juegos o programas como Word, Excel y PowerPoint. El hardware y software conforma el Yin y el Yan, estas características siempre trabajan de la mano, mientras el software aporta las operaciones, el hardware es el canal físico por el cual dichas funciones pueden realizarse. Aunque aún no tengamos idea de cómo evolucionen las cosas, esta combinación seguirá funcionando como la base del desarrollo tecnológico.

### *Componentes que conforma el Hardware*

Los dispositivos de entrada son aquellos equipos y componentes que permiten ingresar información a la unidad de procesamiento. La tarjeta madre (motherboard) o componente de proceso, también llamada placa base, es una placa con circuitos impresos y soldados que interconectan todas las piezas electrónicas de la computadora. Finalmente, componentes de salida, se conoce como dispositivos de salida (output) a aquellos que permiten la extracción o recuperación de información proveniente del computador o sistema informático, es decir, su traducción a términos visuales, sonoros, impresos o de cualquier otra naturaleza.

### *Componentes que conforma el Software*

El software de aplicaciones incluyen los componentes lógicos, entre muchos otros, las aplicaciones informáticas; tales como el procesador de texto, que permite al usuario realizar todas las tareas concernientes a la edición de textos; el software de sistema, tal como el sistema operativo, que, básicamente, permite al resto de los programas funcionar adecuadamente, facilitando también la interacción entre los componentes físicos y el resto de las aplicaciones, y proporcionando una interfaz amigable con el usuario. Finalmente, software de programación incluyen todas las herramientas que permiten al programador desarrollar programas informáticos, usando diferentes alternativas y lenguajes de programación, de una manera práctica.

### **Taller**

- Identificar los componentes de la computadora
- Encender la computadora
- Iniciar sesión en Windows
- Acceder a Chrome
- Acceder a nuestro correo personal/institucional.

## Capítulo 2

### Copia de respaldo

Los archivos son importantes en un ordenador, de donde se deduce la vulnerabilidad del mismo y se generan copias de seguridad ante distintos problemas que se presentasen. La copia de seguridad se presenta como una herramienta en opción ante sucesos imprevistos que puedan generar perder la información de tu sitio. Los ataques cibernéticos están en el primer lugar de la lista, aunque no son los únicos; diariamente existen miles de intentos para quebrar la seguridad e invadir los portales digitales en todo el mundo. Mantener un sitio web con protocolos de seguridad y realizar copia de respaldo constantemente ayudará a evitar grandes pérdidas y problemas para tu sitio web, empresa, redes y archivos de tal. Los datos, tarde o temprano se perderán por alguna razón: errores del hardware, errores del software, error humano o catástrofe natural. Es por ello, que disponer de copias de seguridad que garanticen la recuperación de la información a un estado anterior es imprescindible.

Una copia de seguridad, respaldo, copia de respaldo, backup o copia de reserva en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos, por ejemplo, recuperar los sistemas informáticos

y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas.

El proceso de copia de seguridad se complementa con otro conocido como restauración de los datos, que es la acción de leer y grabar en la ubicación original u otra alternativa los datos requeridos. Antes de que los datos sean enviados a su lugar de almacenamiento se lo debe seleccionar, extraer y manipular.

Los datos, tarde o temprano se perderán por alguna razón: errores del hardware, errores del software, error humano o catástrofe natural. Es por ello, que disponer de copias de seguridad que garanticen la recuperación de la información a un estado anterior es imprescindible.

Antes de que los datos sean enviados a su lugar de almacenamiento se lo debe seleccionar, extraer y manipular. Se han desarrollado muchas técnicas diferentes para optimizar el procedimiento de efectuar los backups. Estos procedimientos incluyen entre otras optimizaciones para trabajar con archivos abiertos y fuentes de datos en uso y también incluyen procesos de compresión, cifrado, y procesos de des duplicación, entendiéndose por esto último a una forma específica de compresión donde los datos superfluos son eliminados.

### *Areca Backup*

El programa dispone de una interfaz gráfica pero también se puede usar mediante consola de comandos para automatizar las copias. Areca Backup tiene algunas características interesantes como: compresión de archivos (Zip y Zip64), codificación de archivos (Triple DES y AES), almacenamiento en dispositivos portátiles, filtro de archivos para seleccionar qué debe copiarse y qué no, copias incrementales y

diferenciales. Se distribuye bajo licencia GNU General Public License (GPL). Podemos filtrar los archivos a ser copiados por extensión, subdirectorio, expresión regular, tamaño, fecha o estado.

No sólo genera copias de seguridad de nuestro disco duro sino también de dispositivos USB, archivos en red y servidores FTP.

Areca usa el tamaño y la fecha de última modificación para detectar archivos modificados. Esto permite una rápida detección de archivos modificados. Funciona en cualquier sistema operativo, siempre que tenga Java Runtime Environment instalado (versión 1.4.2 o superior). Características del aplicativo:

- Compresión de archivos (formato Zip).
- Archivos de cifrado (Triple DES y AES algoritmo de cifrado).
- Filtros de archivo de origen (por extensión, subdirectorio, expresión regular, tamaño, fecha, estado, uso).
- Incrementales / copia de seguridad completa de apoyo
- Archivos fusiona / eliminación: Es posible combinar los archivos contiguos en un solo archivo o eliminar sus archivos más recientes.
- A partir de la fecha de recuperación: Areca le permite recuperar sus archivos (o archivos individuales) a partir de una fecha concreta.
- Mecanismo de transacción: Todos los procesos críticos (tales como copias de seguridad o se fusiona) apoyo a un mecanismo de operación (con commit / rollback gestión) las copias de seguridad que garantiza su integridad.
- Copia de seguridad de informes: Areca genera informes de copia de seguridad que se pueden almacenar en su disco o enviar por correo electrónico.
- Publicar los scripts de copia de seguridad: Areca puede lanzar scripts de shell después de copia de seguridad.
- Los permisos de los archivos de copia de seguridad. (Linux solamente)

- Explorador de archivos de contenido. (incluyendo un "encontrar el archivo en los archivos" característica)
- Archivo de descripción: un manifiesto está asociado a cada archivo, que contiene diversas informaciones, tales como autor, título, fecha, descripción, y algunos datos técnicos.
- Archivo de la historia del explorador: Areca realiza un seguimiento de su expediente de la historia (creación / modificación / supresión) en sus archivos.
- Copia de seguridad de la simulación: tiempo útil para comprobar una copia de seguridad es necesario
- Acciones del usuario historia: Areca mantiene un historial de todas las acciones del usuario (archivos de supresión, se fusiona, backups, recuperaciones).
- Archivo de indicadores: Areca calcula una gran cantidad de indicadores para usted, que le ayudará en la gestión diaria de sus archivos.
- Areca viene con una interfaz de línea de comandos que pueden ser utilizados para la automatización de copia de seguridad.

### *Cobian Backup*

Es un programa multitarea capaz de crear copias de seguridad en un equipo, en una red local o incluso en/desde un servidor FTP. También soporta SSL. Se ejecuta sobre Windows y uno de sus grandes fuertes es que consume muy pocos recursos y puede estar funcionando en segundo plano.

Cada tarea de respaldo que le asignemos puede ejecutarse en el momento, diaria, semanal, mensual o anualmente, o en un tiempo especificado. Hace copias completas, incrementales y diferenciales.

Soporta compresión ZIP, Zip64 o SQX. Además, ofrece la opción de proteger todas las funciones del programa por contraseña. Existe la opción de cifrar sus ficheros usando 4 métodos diferentes de cifrado fuerte: RSA-Rijndael (1024-256-bits), Blowfish (128-bits), Rijndael (128-bits) o DES (64-bits).

También pueden definir eventos disparados antes o después de la copia, como por ejemplo provocar el cierre de un determinado programa que utilice un fichero que se va a copiar y hacer que una vez finalizada la copia se vuelva a iniciar.

Más allá del backup, Cobian Backup puede utilizarse como programador de tareas, ejecutando determinadas aplicaciones cuando lo deseemos.

### *Mendeley*

Es una aplicación web y de escritorio, propietaria y gratuita. Permite gestionar y compartir referencias bibliográficas y documentos de investigación, encontrar nuevas referencias y documentos y colaborar en línea. Mendeley combina Mendeley Desktop, una aplicación de gestión de referencias bibliográficas y de documentos en formato PDF (disponible para Windows, Mac y Linux) con Mendeley web. Ambas aplicaciones son la base sobre la cual se ha creado y desarrollado una red social en línea de investigadores.

### *One Drive, Dropbox, Box, Google Drive y Icloud*

Los servicios de almacenamiento en la nube han prosperado en los últimos años y actualmente hay una oferta muy variada y completa. Compañías como Google, Apple o Microsoft ofrecen servicios propios, que compiten con iniciativas independientes como Dropbox o Box. La oferta de todos ellos consiste en almacenar contenidos como documentos o fotografías en servidores remotos, pero sus tarifas y sus posibilidades varían. Los



interesados en aprovechar el potencial de la nube deben conocer las características de cada servicio para decantarse por uno u otro. Todos los servicios permiten a los usuarios buscar, ver y organizar archivos almacenados, además los miembros del grupo pueden acceder, crear, modificar y eliminar archivos dentro de las carpetas de cada uno de los servicios

## Capítulo 3

### Herramientas básicas

#### *Microsoft Word*

Es una de las herramientas de procesador de textos más potentes del mercado para un usuario medio. Sin lugar a dudas, en su versión 2019, sigue siendo el mejor procesador de textos, es prácticamente invencible. Sigue siendo cómodo para la redacción de cartas, documentos, ensayos e incluso para preparar boletines informativos. A pesar de la gran cantidad de características y herramientas, la aplicación aún se presenta como accesible e intuitiva, gracias a la interfaz gráfica de usuario, compuesta de una banda en la parte superior de la ventana donde se expone los objetos (Ribbon). Ha mejorado las opciones de traducción, conversión de texto a voz y espaciado de texto, así como un mejor soporte para lápices y dibujos digitales dentro de tus documentos. También es nuevo, un modo de enfoque que elimina las distracciones que lo rodean cuando necesitas leer algo en la pantalla.

*Inicio de Word*

En Windows 10, al hacer clic en el botón Inicio se muestra el menú Inicio. En ese menú, puede elegir la aplicación que desea iniciar usando el mouse o, si tiene un monitor de pantalla táctil, pulsando la aplicación que desee iniciar. El menú Inicio proporciona acceso a correo, OneDrive, Microsoft Edge, fotos, juegos, música, video y, por supuesto, la última versión de las aplicaciones de Microsoft Office. En las tabletas con Windows Mobile y las aplicaciones de Office 2019 instaladas, puede personalizar la interfaz del mismo modo que el menú Inicio.

Aunque no tenga Office 2019 instalado en su dispositivo informático, puede crear, ver y realizar ediciones sencillas en documentos de Word mediante una Word Web App en línea. Hay disponibles aplicaciones web de Office para Word, Excel, PowerPoint y OneNote. Para iniciar Office Web Apps se utiliza un explorador web, como Microsoft Edge. Una de las diferencias entre la aplicación web de Word y la aplicación Word 2019 instalada en su equipo es el número de funciones disponibles.

La Word Web App le permite crear, abrir y editar documentos solamente con los comandos más básicos. Es una manera maravillosa de crear un documento sencillo y compartirlo. La principal ventaja del uso de la aplicación de Word 2019 instalada en su equipo consiste en que tiene acceso completo a todas las funciones necesarias para crear un documento de aspecto profesional. Si utiliza la Word Web App, no podrá completar todos los ejercicios de este libro, porque esta no incluye todas las funciones de Word.

Microsoft tiene un espacio para el almacenamiento basado en la nube conocido como OneDrive. Microsoft brinda a los usuarios espacio gratuito para el almacenamiento remoto, lo cual les permite administrar sus documentos desde cualquier lugar y compartirlos con quien deseen. Sin embargo, para poder usar OneDrive, necesita crear un perfil de cuenta de Microsoft. Una vez creada la cuenta, le resultará fácil administrar y compartir sus documentos.

Windows 10 trabaja sin problemas con Office 2019. Una vez que inicie sesión en su cuenta de Microsoft, el nombre de la cuenta aparece en el

extremo superior derecho de cada aplicación de Office 2019 y usted tiene acceso a los archivos que haya almacenado en su espacio de OneDrive.

Esto hace que sea más fácil para usted seguir trabajando en sus documentos en cualquier equipo y le recuerda dónde los dejó.

Para comenzar a usar Word 2019, ubique el icono de Word y haga clic en él con el botón primario del mouse o, si está utilizando un monitor de pantalla táctil, pulse el icono.

Cuando se inicia Word, el programa se abre con la pantalla de Word 2016. En el lado izquierdo de la pantalla, bajo Reciente, verá una lista de documentos a los que se ha tenido acceso recientemente. El panel de la ventana derecha muestra una página de documento en blanco y varias plantillas para crear documentos personalizados. Para crear un documento en blanco, haga clic en la página de Documento en blanco y Word abrirá un documento nuevo.

### *Microsoft Excel*

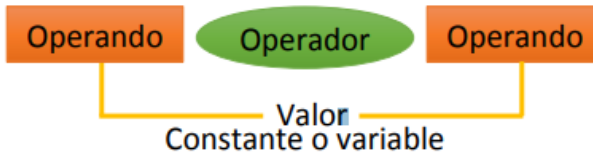
Excel es uno de los programas de Microsoft más usado en el mundo, ya que sirve para realizar cálculos numéricos o matemáticos, pero si conoces todos los trucos que oculta este programa, será mucho más fácil su uso. En la hoja de cálculo se pueden registrar números, datos y texto. Pero Excel tiene funciones muchas más amplias y puedes realizar desde una simple suma, hasta resolver integrales, crear gráficos, ordenar y agregar información no numérica, resolver programas matemáticos y muchos más si sabes los trucos que tiene este programa. Ningún otro programa de hoja de cálculo se acerca realmente a Excel en términos de capacidades avanzadas. En su nueva versión 2019 tienes mejoras similares a las capacidades de entintado, así como algunas nuevas funciones y nuevos tipos de gráficos. Ahora también puedes colocar modelos 3D en tus hojas de cálculo y verlos desde todos los ángulos.

Excel es un sistema de hojas de cálculo, esto es, de planillas de gestión de información de manera ordenada y sistemática, permitiendo la automatización de operaciones lógicas (aritméticas, geométricas, etc.) y

facilitándole la vida a los contadores, financieros, gestores de información e incluso a quienes trabajan con listas. Se trata de una aplicación versátil, útil sobre todo para elaborar tablas, gráficas y otras operaciones de representación de la información, a partir de una matriz virtualmente infinita de filas y columnas en las que pueden introducirse y personalizarse los datos. Además, Excel cuenta con un sistema de macros o fórmulas automatizadas, que permiten también su empleo con fines de algoritmos.

### Expresión

Es un conjunto de constantes, variables y operadores con los cuales se realiza las operaciones para obtener un resultado.



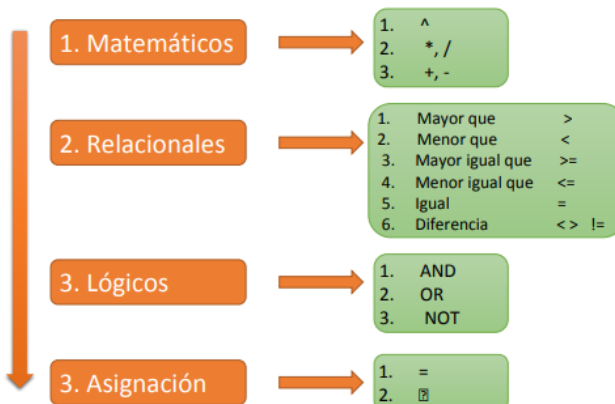
### Ejemplo:

$$\text{resultado} = a - (3 * b + 6) / c$$

### Operando

Es el valor que interviene de variables y/o constantes.

### Tipos de Operadores (Jerarquía)



### Pasos para crear una fórmula

1. Seleccionar la celda para ingresar la fórmula.
2. Anteponer el signo = ya que de esta forma se le indica a Excel de que se trata de una fórmula, de lo contrario, lo toma como texto.
3. Se introducen los valores y la operación que se va a realizar. Los valores pueden ser escritos o hacer referencia a la celda que los contiene.

SUMA		RESULTADO	ó	SUMA		RESULTADO
10	15	=10+15		10	15	=D6+E6

#### 4. Presionar Enter para obtener el resultado.

SUMA		RESULTADO
10	15	25

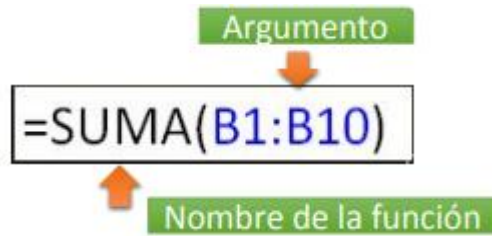
### Funciones

Las funciones son formulas predefinidas que tiene la hoja de cálculo Excel y que al igual que las fórmulas inicia con el signo = y permiten realizar cálculos precisos, pero minimizando la complejidad de las operaciones. La hoja de cálculo Excel cuenta con categorías y estas a su vez con otras, por lo que existe una gran variedad de funciones.

1. Financieras.
2. Fecha y hora
3. Matemáticas y trigonométricas.
4. Estadísticas.
5. Búsqueda y referencia.
6. Base de datos.
7. Texto.
8. Lógicas.
9. Información.
10. Ingeniería.
11. Cubo.
12. Definidas por el usuario.

### Elementos de una función

1. Nombre de la función que permita identificarla.
2. Estructura: Después del nombre de la función, se abre paréntesis para los argumentos de la función y se cierra paréntesis.
3. Argumentos: Son los valores y estos pueden ser de texto, numéricos, referencias de celdas, etc.



### *Microsoft PowerPoint*

Microsoft ha anunciado una nueva herramienta para PowerPoint que utilizará la inteligencia artificial para hacer sugerencias al usuario durante la exposición de sus presentaciones, indicándole si está utilizando frases que pueden herir la sensibilidad en determinadas culturas o si está leyendo demasiado la diapositiva, entre otros aspectos. Microsoft ha presentado también la introducción de varias herramientas de diseño para PowerPoint que utilizan la inteligencia artificial para hacer recomendaciones de diseño al usuario en la creación de sus presentaciones. Todos conocemos las ventajas de esta herramienta de presentación de proyectos, realmente todopoderosa. Pero en su versión Office 2019, nos presenta algunos trucos nuevos, como el soporte para avanzar diapositivas con plumas Bluetooth, una nueva interfaz de zoom para saltar entre diapositivas y una transición de morfología fresca.

Recomendaciones para crear presentaciones originales y muy profesionales:

1. Disponer de imágenes atractivas y de calidad.
2. Elección del diseño (colores, tipografías, etc.), nuestro diseño deberá coincidir exactamente con el tipo de comunicación que quieres transmitir.
3. Define bien el timing (el tiempo de cada dispositiva).

4. Más visual menos texto, una presentación es un documento que nos sirve de apoyo para nuestra exposición.

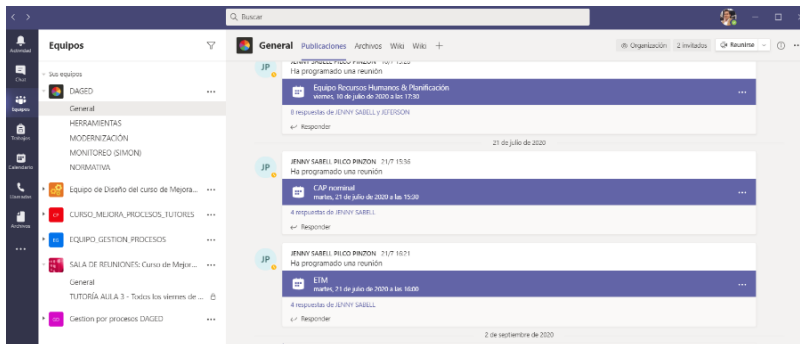
5. Realizar una presentación en 20 minutos.

6. Incluye vídeo para hacer tu presentación más dinámica.

Otros programas alternativos son Canva, Visme, Adobe Spark, LibreOffice Impress, Zoho Show, Prezi, Emaze, Knovio, PowToon, Genial, Sway y VideoScribe

### *Aula virtual*

La formación ha ido evolucionando hacia nuevos entornos de aprendizaje denominados e-learning (educación en línea). A través de diferentes herramientas y plataformas, actualmente, podemos generar de manera sencilla nuestra propia aula virtual. Un ejemplo para crearla es Microsoft Teams, una aplicación dentro de Office 365 que permite gestionar equipos, clases, proyectos, etc.





Classroom es un servicio gratuito para escuelas, ONG y cualquier persona que tenga una cuenta de Google personal. Classroom facilita la conexión entre profesores y alumnos, tanto dentro como fuera de la escuela; Permite ahorrar tiempo y papel, así como crear clases, distribuir tareas, comunicarse con otros usuarios y mantener el trabajo organizado con facilidad.



## Capítulo 4

### Formularios Digitales

Los tiempos cambian rápidamente y sobre todo las empresas deben encontrar la manera de adaptarse a los clientes y el mercado de manera que sigan siendo competitivas. Los empresarios siempre están intentando maximizar sus recursos, optimizar sus operaciones y hacer que sus negocios sean más rentables y para lograrlo deben encontrar métodos eficientes para compilar datos y convertirlos en información útil para mejorar sus gestiones. Para tomar las decisiones correctas es necesario procesar y evaluar grandes volúmenes de datos. Y es ahí donde el rol de los formularios digitales adquiere importancia, ya que permiten obtener resultados más precisos y de una manera más rápida que usando los tradicionales formularios de papel.

Tradicionalmente se usaban encuestas por correo, entrevistas telefónicas y entrevistas puerta a puerta para acceder a la información. Con la llegada de la digitalización, estos procedimientos han sido reemplazados por otros métodos más sofisticados y efectivos.

La transformación digital está cambiando la manera de hacer negocios y la forma de realizar investigaciones y estudios de mercado. Muchas operaciones que antes se ejecutaban manualmente hoy se realizan utilizando métodos digitales. La tecnología ha tenido un gran impacto en

la forma de abordar las investigaciones de mercado y la recopilación de datos y ha proporcionado a los investigadores nuevas herramientas que han modernizado estos procesos.

La recopilación de información mediante formularios digitales es un paso hacia el futuro porque facilita la recopilación, entrada y análisis de datos, proporcionando resultados más precisos en menos tiempo.

### *¿Qué es un formulario digital?*

Un formulario Online es un documento digital que se inserta en una web o en un email y busca recoger datos del destinatario de manera ordenada. Los formularios son muy útiles para crear una buena base de datos, limpia y actualizada. Es el método más utilizado por las empresas para conseguir posibles clientes o simplemente contactos interesantes.

El formulario online supone un gran avance ante el formulario en papel tradicional, donde había que meter cada contacto uno por uno en tu base de datos. Ahora, con un programa que recoja los datos recibidos todo es más rápido.

Los formularios también te permitirán solicitar información sobre la empresa o novedades, recoger datos para concursos o una encuesta. Los tipos de formularios que podemos clasificar son:

- **Concurso:** Es uno de los formularios más populares. Crea una serie de preguntas y unas posibles respuestas, el usuario los rellenará y, dependiendo de si las respuestas son acertadas o no, ganará un premio relacionado con la empresa.
- **Sorteo o promoción:** El sorteo es una variante del “concurso” solo que es al azar, sin responder a ninguna pregunta en concreto. A través de algún cupón o alguna condición de parte de la empresa, los usuarios entran en el sorteo de un producto.
- **Suscripción:** Es el formulario más clásico y más utilizado. Prácticamente todas las webs tienen un formulario pequeño colocado en la parte superior, donde te invita a suscribirte a la página web para recibir el boletín con las noticias y las novedades de la empresa.

- Empleo: El fin de este formulario es el de obtener los datos de usuarios que quieran trabajar con la empresa. Esto es bueno tanto para la empresa como para el usuario ya que elimina barreras y es rápido.
- Contacto: Es uno de los más comunes, facilitar la comunicación de la empresa y el cliente de manera que es útil crear un formulario de contacto para que el cliente se comuniquen con ellos. De manera que el empresario realice una retroalimentación al cliente, saber que piensa, que siente, si le gusta tu producto, que cambiaría.
- Encuesta: Otro de los formularios más utilizados por los usuarios, la encuesta. Se crea cuando quieres saber una información concreta de tu producto, servicio, de la empresa o del propio cliente.
- Pedido: Este formulario es más propio de tiendas online o de webs que vendan algún artículo en concreto. Se trata de crear un formulario que sea como una factura, como una lista de la compra donde eliges lo que quieras, la talla, el color.
- Evento: Este formulario es menos utilizado Cuando celebre sus eventos o sus talleres se hace describe la información sobre la comida, la asistencia, los asientos o el alojamiento.
- Invitación a una fiesta: Puedes crear una invitación a tu fiesta a todos tus amigos con una serie de campos de interés para ti que han de rellenar. Campos como asistencia, comida que prefieren, datos de interés.

*¿Cómo los formularios digitales pueden beneficiar a tu negocio?*

✓ **Ahorro de tiempo y dinero**

La administración y transferencia de información recopilada a través de encuestas en papel es un proceso lento y engorroso. Con la recopilación automatizada de datos, no necesitas invertir tiempo y recursos en entradas de datos manuales porque el software identifica, selecciona y procesa los

datos automáticamente. De esta manera permite reducir los costos operativos. Además los formularios digitales pueden ser distribuidos masivamente usando plataformas de correo electrónico o a través de redes sociales.

### ✓ **Mejora la efectividad y la precisión de los datos**

Los formularios digitales pueden rellenar automáticamente los campos usando datos ingresados previamente y permiten, además, validar la información ingresada antes de ser enviada. La recopilación de datos digitales también elimina errores de entrada y la pérdida de datos que puede producirse durante la transcripción. Los formularios digitales permiten, asimismo, rastrear y guardar el nombre del usuario, la geolocalización y la hora en que la información fue enviada.

La información recopilada mediante formularios digitales es más precisa y completa que la recopilada mediante formularios impresos, ya que el proceso digital reduce significativamente los errores manuales.

### ✓ **Informes en tiempo real**

En una plataforma digital, los datos pueden ser revisados y analizados luego de haber sido enviados y subidos al servidor, permitiendo a tu empresa generar informes a un ritmo mucho más rápido. Los formularios digitales también brindan la flexibilidad de modificar la encuesta de acuerdo con los comentarios recibidos en tiempo real.

## *Aplicaciones para crear formularios online*

Google Forms es una aplicación de google drive, siendo probablemente la utilidad para crear formularios online más conocida, gracias a su estupenda integración con otras herramientas de esta suite ofimática online, en la cual se puede realizar formularios, encuestas para adquirir estadísticas sobre la opinión de las personas, planificar eventos, hacer preguntas a tus estudiantes o recopilar otros tipos de información de forma fácil y eficiente.

Microsoft Forms es una nueva aplicación de Office 365 que permite a los docentes crear cuestionarios, encuestas y registros personalizados, es una aplicación sencilla y ligera que te permite crear encuestas, cuestionarios y sondeos fácilmente los cuales se podrán compartir para que otros usuarios respondan utilizando cualquier navegador o dispositivos móviles. A medida que se envían los resultados, podrá usar análisis incorporados para evaluar las respuestas. Los datos de formulario, como los resultados de cuestionarios, pueden exportarse fácilmente a Excel para realizar análisis adicionales o asignar notas. Para utilizar la aplicación Forms, debemos iniciar sesión con nuestra cuenta institucional de Office 365.

Formdesk es una herramienta para crear formularios online con docenas de características para ayudarte a diseñarlo y a gestionar la información recogida, y ayudar a los usuarios a interactuar con él (aunque no todas las opciones están disponibles en el plan gratuito). Entre otras cosas, podrás validar los datos de algunos campos (como por ejemplo, números de teléfono), permitir la subida de ficheros, dividir el formulario en varias páginas, generar estadísticas con los datos recopilados, recaudar pagos online, o hacer uso de datos ya introducidos para rellenar el formulario automáticamente.

JotForm es una herramienta online que nos permite crear formularios de forma muy simple, sin la necesidad de codificar ni una línea. JotForm incluye una amplia selección de plantillas de formulario y temas de diseño listos para usar, tiene soporte para plug-ins que le añaden funciones adicionales, e incluso permite gestionar procesos de pago a través de Paypal y otros servicios similares.

Cognito Forms es un Software de Forms Automation Software creado por la empresa Cognito Apps (United States). Es un avanzado generador de formulario en línea que cuenta con una interfaz intuitiva, fácil de usar y el más robusto conjunto de características libres en el mercado. Diseñado desde el principio para la Internet de hoy, la plataforma ofrece características muy potentes; incluyendo documento de fusión, la carga de archivos, la repetición de secciones, ahorrar y hoja de vida, la lógica condicional, y los pagos integrados. Sin problemas incrustar las formas en su sitio web, y recibir una notificación por correo electrónico cada vez que

se presenten nuevas entradas. En Cognito Forms puedes crear tu formulario, publicarlo en tu web o en redes sociales, y gestionar las entradas recogidas, todo ello desde una interfaz web atractiva y fácil de usar.

Formsite, es una herramienta para crear formularios online con una amplia selección de opciones y funciones, Formsite es otra excelente alternativa. Los formularios creados con ella pueden tener hasta 40 tipos de preguntas diferentes, permitir la subida de archivos y procesar pagos online, entre otras cosas. Además son compatibles con dispositivos móviles. En Formsite puedes elegir entre más de 100 plantillas de diseño, y luego adaptarla totalmente al diseño de la página donde irá integrado. Con ellas es posible crear formularios de registro, para campañas de marketing, pedidos online y otras funciones.

Formstack , es un sistema de gestión de datos que ayuda a los usuarios a recopilar información a través de varios tipos de formularios en línea, incluidas encuestas, solicitudes de empleo, registros de eventos y formularios de pago. Los usuarios de Formstack pueden incrustar formularios listos para dispositivos móviles en sus sitios web y perfiles de redes sociales, cobrar pagos en línea, recopilar comentarios de clientes y empleados y crear flujos de trabajo de procesos para su organización.

En la web podemos encontrar otras herramientas que permite recoger la información a través de los formularios, por ejemplo Zoho Forms, Wufoo, iFormBuilder, Formidable Forms y otros.

La manera de avanzar en el marco de la tecnología es cada vez más rápida y necesaria, el uso de los formularios digitales nos proporciona en menor tiempo resultados y recopilación de datos necesarios. La importancia de los formularios digitales radica en que estos a comparación con los formularios de papel nos permiten obtener de manera más rápida y precisa todo tipo de resultados. El uso de un formulario se basa en solicitar información sobre alguna empresa, recoger datos para diversas situaciones como concursos o encuestas.

Existen una variedad de formularios digitales; entre ella la más utilizada y conocida es Google Forms. Los formularios se pueden usar en diversos ámbitos como: educativa, social, empresarial, laboral, social, etc.

## Capítulo 5

### Antivirus y Malware

Al igual que ha sucedido con la tecnología, los virus han evolucionado paralelamente, adaptándose a las formas de comunicación y transmisión más actuales. Pero, ¿Qué es realmente un virus? ¿Cómo afectan? ¿Qué tipos de virus nos encontramos? ¿Tenemos defensas contra ellos? Estas y muchas más preguntas iremos respondiendo mediante avancemos con la investigación.

Primero que nada, necesitamos saber ¿Qué es un virus y un antivirus?

Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad como el gusano informático, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos,



desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

En informática los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos, nacieron durante la década de 1980.

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkits, etc.

### *Malware*

Malware significa software malicioso y viene del inglés malicioso software. Dicho software malicioso es creado para introducirlo en ordenadores ajenos: dañarlos, obtener información de ellos o utilizarlos de forma remota. Todo ello, por supuesto, sin autorización del usuario. El término malware, abarca desde los antiguos virus informáticos hasta el software malicioso, cada vez más sofisticado. Básicamente, bajo la denominación de virus se ha designado cualquier aplicación que modifica a otras, escribiendo o alterando su código, con objeto de realizar alguna acción significativa. Esta idea como tal se toma de la definición propia de un virus biológico. Sin embargo, el virus electrónico ha trascendido mucho más allá de aquella idea original. Ya no se habla solamente de programas que cumplen esta función condicional de replicarse, sino que queda exportada a una categoría de aplicaciones denominada malware (malicioso software). Estos programas tienen como objetivo realizar o desencadenar alguna

acción que provoque un "daño" a la máquina expuesta. Siguiendo esta condición, los troyanos, spyware, keylogger y demás fauna que pululan entre nuestros ordenadores quedan encuadrados junto con los virus entre los programas maliciosos. Algunas veces las líneas divisorias que determinan si un programa es dañino, no quedan demasiado definidas, por ejemplo, una "cookie" que originalmente podemos considerar como inofensivo, pueden convertirse en una trampa mortal para un usuario desprotegido, al igual que puede pasar con los "jokes" (programa broma).

### *Tipos de Malware*

#### **Troyanos**

Los troyanos, al revés que los virus, no provocan daños en las máquinas anfitrionas. Su función es entrar en la máquina sin ser advertido de tal manera que levante la menor sospecha posible para así de esta forma conseguir información o controlar la máquina. Se propagan a través de internet por aplicaciones como el chat, ICQ o el correo electrónico. Los troyanos son especialmente peligrosos porque pueden comprometer la seguridad de un sistema abriendo puertos de comunicaciones, enviando contraseña por correo electrónico, etc. Un troyano puede eliminar la seguridad de nuestro sistema y dejarlo totalmente vulnerable. Un troyano no suele tener la misma finalidad que un virus aunque mucha gente lo considere un tipo de virus pero sigue siendo un malware peligroso. Existen troyanos que son recolectores de contraseñas, están esperando que el usuario teclee alguna cadena de caracteres en un campo etiquetado como contraseña para luego enviarlos por correo electrónico. El troyano puede recolectar contraseñas o bien números de tarjetas de crédito, incluso existen troyanos que modifican los permisos de los usuarios del sistema. En ocasiones habilitan cuentas dándoles los mismos permisos e incluso superiores que el administrador del sistema. Puede llegarse el caso incluso que el propio troyano elimine los privilegios de administración del administrador. De esta forma, el atacante puede hacer y deshacer cuanto quiera en nuestro sistema. El potencial de un troyano es sumamente destructivo puesto que una vez toma control del sistema puede destruir información, inutilizar el sistema operativo, encriptar archivos, etc.

Los troyanos pueden estar divididos en dos sitios: El servidor que se encargará de enviar al cliente las acciones a ejecutar. El cliente que es alojado en la máquina anfitriona se encargará de realizar las acciones que le indique el servidor. Algunos troyanos tienen una librería en el cliente (con extensión .dll). Existen troyanos que permiten al cracker modificar su funcionalidad mediante el editserver o sistema de configuración, que para esa manera el ordenador de las víctimas haga lo que quiera el cracker.

## Keylogger

Sin lugar a dudas un virus es peligroso, pero al final de una u otra forma eres conocedor de su existencia y puedes poner un remedio (o al menos intentarlo). Pero ¿qué pasaría si algo en la máquina estuviera recogiendo lo que hacemos y lo enviara a otra persona? Por supuesto las repercusiones serían mucho más graves. El espionaje informático es una operativa lucrativa utilizada por algunos hackers y que supone un gran peligro. Imaginamos que una persona conoce cada golpe de teclado que realizamos en nuestra máquina. Conocería nuestras password, tendría acceso a nuestro correo, sería capaz de predecir nuestras acciones, detectaría y anticiparía nuestros modos de operación, tendría acceso a toda nuestra información, etc. Los keylogger son aplicaciones malware que tienen este objetivo.

Esta aplicación normalmente llega al usuario de forma camuflada, algo similar a como sucede con los troyanos, y una vez instalado en la máquina ejecuta las acciones correspondientes para recoger cada pulsación que se produzca en el teclado del ordenador. Algunos sitios web (principalmente bancos) conocedores de estos programas han rediseñado sus accesos para introducir las claves de acceso a través de números que son pulsados por ratón en una consola de la página web. Para sobreponerse a estas técnicas los keylogger han ido evolucionando, recogiendo también las comunicaciones de los navegadores y almacenando las pulsaciones de ratón e intentando identificar en qué posición de pantalla fueron accionadas.

Un problema al que se enfrenta un atacante que utiliza un programa de este tipo es la de recoger la información obtenida. Algunos de ellos vuelcan la información en un texto plano y el hacker debería tener acceso físico al mismo para recoger lo obtenido, pero los más avanzados pueden ser

configurados para reenviar la información vía correo a un buzón específico, o establecer una comunicación contra una dirección IP y enviar los datos necesarios. KGB Keylogger presenta estas funcionalidades.

Algunos de estos programas han pasado a ser comerciales y se ha extendido su uso para el control y predicción de acciones. Algunos padres los utilizan para conocer qué lugares de Internet visitan sus hijos, que conversaciones mantienen a través de Messenger, etc.

## Spyware

Basado en conceptos propios de los virus, el spyware es un paso más en los programas maliciosos. Básicamente son programas que están diseñados para recopilar información de los hábitos de visitas a páginas Web de los usuarios.

Al igual que los troyanos, el spyware se instala en los sistemas oculto en software que a simple vista puede ser inofensivo como programas shareware o freeware que el propio usuario ha descargado de la red o cookies que se han descargado después de haber visitado una página web aparentemente inofensiva. Del mismo modo que un virus, se instalan en el sistema sin permiso del usuario.

Entre las acciones que llevan a cabo los programas spyware está la identificación de las visitas a páginas Web, apertura de ventanas anunciando productos o servicios relacionados con lo que se está visitando (Pop-ups), y en los peores casos registros de las pulsaciones de teclado del usuario para robar contraseñas y números de cuentas de tarjetas de crédito (keyloggers).

Como efecto colateral el sistema comienza a sufrir con múltiples procesos abiertos que pueden llegar a colapsar la capacidad del procesador. La experiencia del usuario cada vez se deteriora más hasta que resulta casi imposible ejecutar cualquier programa.

Con la adquisición de Giant Company Software, Inc. [Ver GIANT] Microsoft pretende cubrir una de las mayores necesidades de sus clientes y usuarios finales, la protección contra el Spyware incluida en los sistemas operativos Microsoft Windows. Giant Company Software, Inc. es una

compañía líder en desarrollo de productos de protección y seguridad en Internet. Está localizada en Nueva York y tiene oficinas en Chicago y Atlanta.

El nuevo producto se llama Microsoft Windows Anti-Spyware y actualmente está en versión beta, con una actualización del 16 de febrero de 2005, en la cual se han mejorado los agentes de protección en tiempo real, se han añadido nuevas categorías de amenazas y se ha mejorado la estabilidad y el rendimiento de la aplicación. El número de compilación de la actual versión es 1.0.509.

Además, Microsoft ha puesto en marcha el servicio SpyNet™, el cual es una comunidad mundial de usuarios de Microsoft Windows Antispyware que juegan un papel clave en la determinación de qué software es clasificado como spyware.

No debemos menospreciar el spyware y dejarlo a un lado a la hora de planificar la protección de sistemas de información, servidores y estaciones de trabajo. Hasta los más precavidos administradores pueden verse infectados por spyware sin apenas darse cuenta.

Es recomendable, por lo tanto, no visitar sitios web dudosos o susceptibles de contener spyware, tampoco utilizar sistemas de intercambio de ficheros y redes peer to peer, no abrir correos spam o cuyo remitente no es conocido y además formatear y reinstalar el sistema con cierta regularidad. Tratemos de tomar todas las medidas de protección necesarias. Aun así, cada vez que se ejecute alguna herramienta de detección de spyware nos llevaremos alguna sorpresa al comprobar que de alguna u otra forma ahí están.

### **Adaware**

El adaware o Advertising-Supported software (software financiado con propaganda) consiste en que un software durante su ejecución muestra publicidad sobre productos, servicios, etc. En ocasiones la publicidad permite la financiación del desarrollo y modificación del software que de otra forma desaparecería al no encontrar el programador ningún tipo de

beneficio. En otras ocasiones el objetivo de estos programas es mostrar ventana o publicidad molesta para el usuario sin ningún tipo de beneficio para el mismo (todo lo contrario) y en este caso se consideraría un malware.

### **Botnets**

Conocidas como redes zombies, son redes de ordenadores infectadas, generalmente para utilizarlas de forma remota enviando Spam de manera masiva y anónima.

### **Cookies**

Las cookies son ficheros que se almacenan en el equipo del usuario y sirven para anotar y recordar información del usuario. El usuario en todo momento puede activar o desactivar el uso de estas cookies en las opciones de su navegador. No obstante, es posible que la información de las cookies se utilice con la finalidad de crear perfiles de usuarios sin que los mismos usuarios tengan el conocimiento de ello para luego ser utilizados para enviar publicidad a los mismos o simplemente venderlos a otros sitios u organizaciones.

### **Backdoor**

Backdoor o puerta trasera es un software que permite acceder al sistema saltándose los procedimientos habituales de identificación de tal manera que no se detecte este intrusismo. En ocasiones se produce un cambio en el software de forma malintencionada para crear un backdoor y así poder saltarse la seguridad del sistema.

## **Ramsonware**

El ransomware es un malware que se propaga normalmente como un gusano y su objetivo es inutilizar el sistema o impedir al usuario el acceso a sus ficheros para luego pedir una recompensa por su liberación.

## **Phising**

El objetivo de este malware es suplantar una entidad oficial y obtener de manera fraudulenta información confidencial del usuario, como datos bancarios o contraseñas. Usualmente utiliza como medias páginas web falsas de similar apariencia a las originales, correo electrónico, etc.

## **Web Bug**

Un web bug es una imagen de tamaño muy pequeño (a veces un solo pixel) o invisible que se envía incrustada en una página web o email el cual permite saber si dicha imagen ha sido descargada (el usuario al leer el email o acceder a la página web descarga la imagen). Mediante este sistema se puede conocer si la página web ha sido descargada o el email leído. Por ejemplo, en un correo electrónico el emisor puede conocer si ha leído el correo, cuando y donde lo ha leído. Otras formas de llamar al web bug son: Pixel tag, tracking pixel, tracking bug y Web beacon.

## **Gusanos o Worms**

Un gusano es un malware residente en memoria que no modifica los archivos, pero se va replicando de forma incontrolada, de tal manera que el sistema se ralentiza progresivamente debido al consumo de los recursos llegando en ocasiones a no poder ejecutar procesos normales. Los gusanos calculan las direcciones de otros equipos conectados a la red y envían copias suyas propagándose de este modo. Los gusanos suelen provocar problemas en la red consumiendo ancho de banda propagándose entre los equipos que estén interconectados mediante IRC, SMTP u otros métodos.

## Exploit

Es un software que ataca un fallo o debilidad de un sistema. No tiene siempre por qué ser un malware dado que puede evidenciar la existencia de agujeros de seguridad en un sistema (para corregirlos), pero si éste va anexo a un malware como un gusano o bien se utiliza para inhabilitar el sistema o provocar fallos el resultado puede ser preocupante.

## Rootkit

Un rootkit es una herramienta software que se utiliza para tomar el control de un sistema y utilizarlo en beneficio propio. Generalmente los rootkits utilizan funciones para borrar huellas y no dejar evidencias de su uso. Una vez ganado el sistema es posible dejar puertas traseras o backdoors para propiciar futuros accesos al sistema o incluso exploits para atacar el sistema u otros sistemas.

## Dialer

Este tipo de aplicaciones se han convertido en un verdadero problema fundamentalmente para el usuario doméstico. Desarrolladas originalmente por los proveedores como un método simple para que los usuarios pudieran conectarse a Internet, sin necesidad de grandes configuraciones. Actualmente, sin embargo, son utilizados en muchas ocasiones para redirigir las comunicaciones de los usuarios con Internet sin que estos tengan una constancia directa de ello.

Desde hace un tiempo ha empezado a proliferar una serie de sitios web preparados para descargar una serie de dialers sobre la máquina objetivo. Estas aplicaciones no se pueden ejecutar sin el consentimiento e intervención del usuario, pero las argucias y engaños empleadas son cada día más sofisticados para hacer caer en la trampa al sufrido usuario. Una vez que el dialer se encuentra instalado, este se encarga de cerrar la conexión que actualmente se encuentra activa y realizar una nueva comunicación a internet al número de teléfono que preestablece el marcador. Curiosamente el número suele coincidir con teléfonos de tarifa



especial como pueden ser los 803. Si el usuario no es consciente de esta situación, toda la conexión hacia Internet se reconducirá a través de esta comunicación. El resultado final se obtiene cuando se recibe la factura telefónica. Un poco tarde.

El problema de este uso "supuestamente fraudulento" es que roza lo legalmente establecido. Se informa realmente de su uso y cuáles son las tarifas para el establecimiento de llamada, aunque se hace de una forma enmascarada utilizando hábilmente la información para no alarmar a la víctima, escapando de esta forma a cualquier medida control, puesto que se cumplen los requisitos mínimos que exige la ley.

La implantación progresiva de la tecnología ADSL inmune a ésta técnica ha minimizado el impacto de estos marcadores. A pesar de ello hay muchos equipos que todavía establecen sus conexiones mediante el marcado telefónico y estos aún pueden verse afectados seriamente. Se recomienda concertar con la compañía de acceso a Internet el control para impedir las llamadas hacia este tipo de números de teléfono o utilizar programas que controlen las llamadas desde el MODEM.

### **Leapfrog o ranas**

Las ranas entran en los sistemas descubriendo cuentas y contraseñas de correo para así de esta manera dar el salto y replicarse en otros sistemas.

### **Jokes**

Aunque no pueden quedar encuadrados directamente en el mismo grupo que virus, troyanos, etc., en cuanto al daño que producen, estas bromas se pueden incluir perfectamente bajo la categoría de malware y no es menos cierto que sus repercusiones pueden ser muy negativas. De aspecto totalmente inofensivo, los programas jokes se han ido distribuyendo mediante correo con el único propósito de gastar una jugarreta a un amigo, aunque a veces ésta llega más lejos de lo normalmente razonable. Imagine a un usuario novato ejecutando una aplicación que le pregunta: ¿desea formatear el disco duro? y aunque se dé la orden de cancelar para que no se inicie el supuesto procedimiento de formateo, éste se inicie, con el consiguiente susto por parte del engañado. Lo más probable en una lógica

reacción va a ser apagar repentinamente el equipo, con la posible pérdida de información.

También en las empresas tienen sus consecuencias perniciosas, especialmente relacionadas con pérdidas de productividad. Normalmente estos juegos acaban con el desplazamiento de un técnico de soporte al puesto de trabajo para evaluar qué es lo que ha ocurrido, intentando solucionar un problema que inexistente.

### **Scumware o escoria**

El scumware es software que realiza varias acciones no deseadas como no permitir ser desinstalado, modificar el funcionamiento de los sitios web como redirigir páginas web hacia otras páginas, crear hiperenlaces no deseados o cambiar los banners de publicidad por otros.

### **Spam**

Se conoce como spam a todos los emails basura que se recibe con múltiples finalidades, desde los emails que muestran publicidad directamente hasta las cadenas con falsas historias de niños con alguna enfermedad, animales abandonados o consejos que tienen que reenviar a "no sé cuántos amigos", para que no te ocurra nada malo.

### **Honeypot**

Son sistemas que simulan ser vulnerables para propiciar el ataque de los crackers y así de esta forma conocer las técnicas y maneras de actuar de los mismos. También sirven a los administradores para distraer a los crackers con máquinas que no son relevantes y de esta forma salvaguardar la seguridad de las máquinas importantes advirtiendo al administrador del problema producido.

### **Spyware enmascarado**

Suelen aparecer ventanas que avisan que el sistema se encuentra en problemas y muestran su ayuda. Cuando se hace caso a estas advertencias lo que ocurre después es que se descarga e instala el spyware sin saberlo.

### *Virus*

Un virus es aquel que altera el funcionamiento del ordenador sin ningún tipo de permiso o conocimiento del propio usuario. Es un programa software que se adjunta contagiando un archivo del sistema para propagarse a otros equipos y dañar el sistema. Dependiendo del tipo de virus las consecuencias para el equipo serán de mayor o menor gravedad (igual que los virus humanos). Nunca hay que abrir correos de desconocidos. La mayoría de virus entran en los sistemas vía correo electrónico. No abrir ni ejecutar ficheros adjuntos si no se conoce a ciencia cierta el contenido de dicho archivo (puede contener un virus).

#### Difusión de los virus

Los virus informáticos se difunden cuando las instrucciones - o código ejecutable - que hacen funcionar los programas pasan de un ordenador a otro. Una vez que un virus está activado, puede reproducirse copiándose en CD/DVD, en el disco duro, en pendrives, en programas informáticos o a través de redes informática. Los archivos más vulnerables a la infección son del tipo .EXE y .COM.

#### Funcionalidad de los virus

Los virus funcionan, se reproducen y liberan sus cargas activas sólo cuando se ejecutan. Por eso, si un ordenador está simplemente conectado a una red informática infectada o se limita a cargar un programa infectado, no se infectará necesariamente. Normalmente, un usuario no ejecuta conscientemente un código informático potencialmente nocivo; sin

embargo, los virus engañan frecuentemente al sistema operativo del ordenador o al usuario informático para que ejecute el programa.

### Su integración

Algunos virus tienen la capacidad de adherirse a programas. Esta adhesión puede producirse cuando se crea, abre o modifica el programa. Cuando se ejecuta dicho programa, lo mismo ocurre con el virus. Los virus también pueden residir en las partes del disco duro o flexible que cargan y ejecutan el sistema operativo cuando se arranca el ordenador, por lo que dichos virus se ejecutan automáticamente. En las redes informáticas, algunos virus se ocultan en el software que permite al usuario conectarse al sistema.

#### 4.1.3 ¿Cómo actúa un virus informático?

Las fases de los virus informáticos son muy parecidas a las fases de un virus biológico. En una primera fase los equipos se infectan y van creándose copias del virus dentro del programa afectando a la configuración y archivos de equipo. Al desarrollador del virus generalmente no le interesa que se den a conocer (que sea observable sus síntomas) puesto que en una siguiente fase de propagación el virus se va a intentar replicar en tantos equipos como pueda. Los virus actualmente se propagan por medio telemáticos (descargando programas, ficheros adjuntos en emails, etc.) aunque también por el uso de pendrives y otros dispositivos de almacenamiento de la información.

La última fase y más letal es la explosión del virus. Es cuando se activa, en ese momento realiza la acción para la cual fue programado. Dependiendo de los efectos que provoque el virus estos serán más o menos devastadores.

Características de un virus que infecta el sector de arranque del ordenador

- ✓ El ordenador no puede lanzar el sistema operativo.
- ✓ El ordenador no puede realizar una configuración basada en disco.
- ✓ El MEM.exe de MS DOS indica 638 KB o menos de memoria base.
- ✓ Recibe errores de disco y no del sistema de la unidad del disco duro.
- ✓ Problemas con la memoria principal y congelación.

### *Antivirus*

Un antivirus es un programa de computadora cuyo propósito es combatir y erradicar los virus informáticos. Para que el antivirus sea productivo y efectivo hay que configurarlo cuidadosamente de tal forma que aprovechemos todas las cualidades que ellos poseen. Hay que saber cuáles son sus fortalezas y debilidades y tenerlas en cuenta a la hora de enfrentar a los virus.

Debemos tener claro que según en la vida humana hay virus que no tienen cura, esto también sucede en el mundo digital y hay que andar con mucha precaución. Un antivirus es una solución para minimizar los riesgos y nunca será una solución definitiva, lo principal es mantenerlo actualizado. Para mantener el sistema estable y seguro el antivirus debe estar siempre actualizado, tomando siempre medidas preventivas y correctivas y estar constantemente leyendo sobre los virus y nuevas tecnologías.

El antivirus normalmente escanea cada archivo en la computadora y lo compara con las tablas de virus que guarda en disco. Esto significa que la mayoría de los virus son eliminados del sistema después que atacan a éste. Por esto el antivirus siempre debe estar actualizado, es recomendable que se actualice una vez por semana para que sea capaz de combatir los virus que son creados cada día. También, los antivirus utilizan la técnica heurística que permite detectar virus que aún no están en la base de datos

del antivirus. Es sumamente útil para las infecciones que todavía no han sido actualizadas en las tablas porque trata de localizar los virus de acuerdo a ciertos comportamientos ya preestablecidos.

El aspecto más importante de un antivirus es detectar virus en la computadora y tratar de alguna manera de sacarlo y eliminarlo de nuestro sistema. Los antivirus, no del todo facilitan las cosas, porque ellos al estar todo el tiempo activo y tratando de encontrar un virus, al instante esto hace que consuman memoria de la computadora y tal vez la vuelvan un poco lentas o de menos desempeño.

Un buen antivirus es uno que se ajuste a nuestras necesidades. No debemos dejarnos seducir por tanta propaganda de los antivirus que dicen que detectan y eliminan 56,432 virus o algo por el estilo porque la mayoría de esos virus o son familias derivadas o nunca van a llegar al país donde nosotros estamos. Muchos virus son solamente de alguna región o de algún país en particular.

A la hora de comprar un buen antivirus debemos saber con qué frecuencia esa empresa saca actualizaciones de las tablas de virus ya que estos son creados diariamente para infectar los sistemas. El antivirus debe constar de un programa detector de virus que siempre este activo en la memoria y un programa que verifique la integridad de los sectores críticos del disco duro y sus archivos ejecutables. Hay antivirus que cubren esos dos procesos, pero si no se puede obtener uno con esas características hay que buscar dos programas por separado que hagan esa función teniendo muy en cuenta que no se produzca ningún tipo de conflictos entre ellos.

Un antivirus además de protegernos el sistema contra virus, debe permitirle al usuario hacer alguna copia del archivo infectado por si acaso se corrompe en el proceso de limpieza, también la copia es beneficiosa para intentar una segunda limpieza con otro antivirus si la primera falla en lograr su objetivo.

En la actualidad no es difícil suponer que cada vez hay más gente que está consciente de la necesidad de hacer uso de algún antivirus como medida

de protección básica. No obstante, en principio lo deseable sería poder tener un panorama de los distintos productos que existen y poder tener una guía inicial para proceder a evaluarlos.

La función de estos programas antivirus es descubrir y eliminar malware. Para ello, emplea una base de datos con los tipos de malware más conocidos con los que comparar cada archivo entrante en el ordenador y si coinciden se conocerá el nombre del virus que ha infectado el archivo y el antivirus pasará a eliminarlo, o si no es posible, ponerlo en cuarentena. Debido al creciente número de malware, resulta conveniente actualizar dicha base de datos cada cierto tiempo. Por otro lado, un antivirus también permite analizar en cualquier momento las distintas unidades de disco del equipo, memorias extraíbles, etc.

### **Técnica del Scannig**

Esta técnica de scanning está en desuso precisamente porque no evita que el sistema sea infectado. Solo actúa a posteriori, cuando el sistema ya ha sido infectado.

### **Técnicas Heurísticas**

Actualmente, los antivirus además de hacer este tipo de comprobaciones monitorizan los programas en busca de comportamientos «sospechosos» propios de virus. El problema de esta técnica es que se puede sospechar de muchos programas que precisamente no están infectados por virus. Lo más común es encontrarse en el mercado antivirus que combinen varias de estas técnicas para proteger el PC. Además, se analiza cualquier tipo de malware, no solo virus (spam, adaware, spyware, virus).

*¿Cómo se elimina un virus?*

La eliminación de un virus consiste en eliminar el archivo que contiene el virus o eliminar el código del virus dentro del archivo infectado. También el antivirus debería poder reparar cualquier daño causado en el equipo por el propio virus. Muchas veces los antivirus no pueden eliminar el código del virus dentro de los archivos y simplemente dan la opción de borrar los archivos infectados. Esto sucede en los casos de virus polimórficos o virus que la empresa desarrolladora del antivirus no tenga bien investigados. En esos casos si la información es de importancia o los ficheros que se van a borrar son ficheros de sistema es mejor comprobar si existe algún antivirus que pueda desinfectar el equipo de forma más eficaz. El borrado del archivo con el virus es una operación eficaz y ya como medida de último recurso y cuando no haya más remedio se aconseja el formatear nuevamente la partición o disco completo restaurando el MBR (Master Boot Record) pues algunos virus se instalan en él. Antes de realizar una operación que consideremos que pueda afectar al funcionamiento del equipo es mejor contactar con el servicio técnico del antivirus que tengamos y contrastar este punto.

*Precauciones para evitar una infección*

Como ya se ha comentado los virus se suelen propagar por medio del correo electrónico. Enviar el contagio al 100% es muy difícil, pero existen muchas maneras de limitar las probabilidades de contagio y no es difícil llevarlas a cabo. Tres de las más importantes precauciones son:

- No abrir correos de desconocidos



- Si no sabemos a ciencia cierta qué contiene un fichero adjunto no descargarlo (incluso si la persona que lo envía es de confianza).
- Tener el antivirus actualizado.
- Evitar leer el correo si es posible desde programas tipo Outlook o similares puesto que la vista previa de los mensajes lee el correo electrónico.
- Leer el correo a través de la red (Gmail, Yahoo!, Hotmail, etc.) de esa manera no estaremos ejecutando nada en nuestro equipo sino simplemente visualizando el mensaje desde el navegador, puesto que estos gestores de correo ya tienen implementados filtros antivirus y de spam.
- Si el texto del asunto nos parece raro o sospechoso el mensaje puede contener un virus.
- Marcar los mensajes spam en el web mail (Correo no deseado).
- No descargar archivos de sitios no confiables.
- Utilizar lo menos posible los pendrives en otros equipos que no sean los nuestros y totalmente desaconsejable utilizarlo en equipos sin antivirus o antivirus no actualizado.
- Evitar instalar software pirata o ilegal. Muchos de estos softwares contienen troyanos y otro tipo de malware.
- No desactivar el antivirus.
- Si sospechamos que tenemos un virus, intentar chequearlo con distintos antivirus para descartar el contagio.

### ¿Residente, o en la nube?

Algunos antivirus actuales funcionan en la nube, en lugar de hacerlo residente en el ordenador local. Esto produce algunas diferencias en el uso y mantenimiento, pero no en los resultados. Ambos modelos son igual de eficientes. Los antivirus residentes se instalan como un programa y deben actualizarse casi todos los días, descargando las nuevas definiciones de virus. Este proceso suele ser automático, así que no supone mayor problema. Los antivirus en la nube funcionan en un servidor de la compañía

de seguridad, en vez de en tu PC. Esto tiene la ventaja de que no necesitas actualizarlos porque siempre están actualizados en el propio servidor remoto. Pero suelen funcionar algo más lento. Por lo demás ambos tipos realizan chequeos similares y funcionan igual.

### **Un antivirus no es suficiente**

Hace años bastaba con instalar un antivirus para mantener tu ordenador a salvo de cualquier amenaza. Hoy en día debes acompañarlo de un software antitroyanos del estilo de Malwarebytes Antimalware, y de un limpiador de disco como CCleaner o equivalente, que borra cookies e historiales, y preserva tu privacidad. Algunos antivirus incluyen una de estas protecciones extra (o las dos), pero no todos. Recuerda también realizar chequeos completos con el antivirus al menos una vez a la semana, para detectar cualquier software malicioso que se pudiera haber colado sin dar la alarma.

#### *Antivirus Online*

Los principales fabricantes de antivirus tienen sitios webs que hacen, sin la necesidad de instalar el software, la comprobación y limpieza de virus en nuestros ordenadores. El funcionamiento es semejante al de los antivirus comunes. Pero, cuidado, el antivirus online no sustituye al común, que te descargas e instalas en tu ordenador. Sirve sólo para una comprobación en el momento.

#### Kaspersky Online Virus Escáner

El Kaspersky Online Virus Escáner utiliza la tecnología Microsoft ActiveX para escanear tu computadora en búsqueda de códigos

maliciosos, ofreciendo la misma tasa de detección de otros productos de Kaspersky Lab.

### McAfee FreeScan

El McAfee FreeScan te ayuda a detectar miles de virus en tu computadora. Basado en el premiado mecanismo de McAfee VirusScan, el FreeScan busca virus (inclusive los más recientes) y muestra una lista detallada de los archivos infectados. Si encuentra virus, el FreeScan nos mostrará unos links con más información sobre el virus y sobre lo que se debe hacer para limpiar el sistema.

### BitDefender

Un antivirus completamente funcional con todos los elementos necesarios para localizar y eliminar los virus de tu ordenador. Es capaz de realizar un escaneo de la memoria, de todos los archivos, carpetas y unidades, además de los sectores de boot. Por defecto, el BitDefender intentará desinfectar los archivos infectados. Si la desinfección falla, los archivos infectados serán eliminados sin aviso. Sin embargo, podrás cambiar esta configuración para que el programa adopte otra medida en el tratamiento para los archivos infectados.

### CA's eTrust Antivirus Web Escáner

El CA's eTrust Antivirus Web Escáner es una manera rápida y fácil de usar herramientas capaces de detectar y limpiar los más recientes virus, worms y troyanos de tu navegador. El software es gratuito, y no necesita componentes adicionales. Todo lo que se solicita para la utilización del scanner web es una conexión a internet, y Microsoft Internet Explorer versión 4 o posterior.

### Trend Micro HouseCall

Trend Micro HouseCall es una aplicación para verificar si tu ordenador fue infectado por algún virus, spyware u otro malware. HouseCall realiza verificaciones adicionales de seguridad para identificar y corregir vulnerabilidades y para prevenir una reinfección.

### ESET Online Escáner

El ESET Online Escáner es un servicio gratuito on-line, simple y rápido, que realiza un rastreo anti-amenazas virtuales. Este servicio ejecuta, a través de un navegador web, un escaneo detallado del ordenador e identifica virus, spywares y otras amenazas virtuales, además de eliminarlas. Este servicio elimina códigos maliciosos sin la necesidad de desinstalar el antivirus actual y posee la misma tecnología ThreatSense (disponible en el ESET NOD32). El ESET Online Escáner no suple la protección en tiempo real, visto que es una herramienta bajo-demanda, que detecta y elimina códigos maliciosos que ya están en tu computadora. Para contar con la protección en tiempo real y permanente es necesario instalar una solución antivirus capaz de asegurar la protección total de tu ordenador y toda la red.

### Panda ActiveScan 2.0

El Panda ActiveScan 2.0 es un avanzado escáner on-line basado en Inteligencia Colectiva que detecta infección de malware que las soluciones de seguridad tradicionales no son capaces de detectar.

### F-Secure Online Escáner

Versión online del antivirus F-Secure (versión 3.3). Es ideal para escanear ordenadores sin antivirus instalados, con las actualizaciones de antivirus desactualizadas o con sospecha de contaminación inclusive con el antivirus actualizado. Utilízala para saber si tu computadora está infectada, y para que lo desinfectes, si es necesario.

## Firewall

También llamado cortafuegos, controla la entrada y salida de agentes sospechosos entre el sistema y la red. Presenta la limitación de no proteger el sistema una vez que el agente ya ha penetrado en él. Posee un sistema de filtro que protege a un ordenador o a una red de ordenadores de entradas no autorizadas contra intrusiones provenientes de redes de terceros (generalmente desde internet). Un sistema de firewall filtra paquetes de datos que se intercambian a través de internet. Por lo tanto, se trata de una pasarela de filtrado que comprende al menos las siguientes interfaces de red:

- Una interfaz para la red protegida (red interna)
- Una interfaz para la red externa.

### ¿Dónde se puede instalar un Firewall?

El sistema firewall es un sistema de software, a menudo sustentado por un hardware de red dedicada, que actúa como intermediario entre la red local (u ordenador local) y una o más redes externas. Un sistema de firewall puede instalarse en ordenadores que utilicen cualquier sistema siempre y cuando:

- La máquina tenga capacidad suficiente como para procesar el tráfico
- El sistema sea seguro
- No se ejecute ningún otro servicio más que el servicio de filtrado de paquetes en el servidor. En caso de que el sistema de firewall venga en una caja negra (llave en mano), se aplica el término "aparato".

### ¿Cómo funciona un sistema de Firewall?

Un sistema firewall contiene un conjunto de reglas predeterminadas que le permiten al sistema:

- Autorizar la conexión (permitir)
- Bloquear la conexión (denegar)

- Rechazar el pedido de conexión sin informar al que lo envió (negar).

Todas estas reglas implementan un método de filtrado que depende de la política de seguridad adoptada por la organización. Las políticas de seguridad se dividen generalmente en dos tipos que permiten:

- La autorización de sólo aquellas comunicaciones que se autorizaron explícitamente: "Todo lo que no se ha autorizado explícitamente está prohibido".
- El rechazo de intercambios que fueron prohibidos explícitamente.

El primer método es sin duda el más seguro. Sin embargo, impone una definición precisa y restrictiva de las necesidades de comunicación.

#### Filtrado de paquetes Stateless

Un sistema de firewall opera según el principio del filtrado simple de paquetes, o filtrado de paquetes stateless. Analiza el encabezado de cada paquete de datos (datagrama) que se ha intercambiado entre un ordenador de red interna y un ordenador externo. Así, los paquetes de datos que se han intercambiado entre un ordenador con red externa y uno con red interna pasan por el firewall y contienen los siguientes encabezados, los cuales son analizados sistemáticamente por el firewall:

- La dirección IP del ordenador que envía los paquetes.
- La dirección IP del ordenador que recibe los paquetes.
- El tipo de paquete (TCP, UDP, etc.).
- El número de puerto (recordatorio: un puerto es un número asociado a un servicio o a una aplicación de red).

*Las reglas del Firewall*

Las direcciones IP que los paquetes contienen permiten identificar el ordenador que envía los paquetes y el ordenador de destino, mientras que el tipo de paquete y el número de puerto indican el tipo de servicio que se utiliza. La siguiente tabla proporciona ejemplos de reglas del firewall:

**Los Puertos Reconocidos**

Los puertos reconocidos (cuyos números van del 0 al 1023) están asociados con servicios ordinarios (por ejemplo, los puertos 25 y 110 están asociados con el correo electrónico y el puerto 80 con la Web). La mayoría de los dispositivos de firewall se configuran al menos para filtrar comunicaciones de acuerdo con el puerto que se usa. Normalmente, se recomienda bloquear todos los puertos que no son fundamentales (según la política de seguridad vigente). Por ejemplo, el puerto 23 a menudo se bloquea en forma predeterminada mediante dispositivos de firewall, ya que corresponde al protocolo TELNET, el cual permite a una persona emular el acceso terminal a una máquina remota para ejecutar comandos a distancia. Los datos que se intercambian a través de TELNET no están codificados. Esto significa que es probable que un hacker observe la actividad de la red y robe cualquier contraseña que no esté codificada. Generalmente, los administradores prefieren el protocolo SSH, el cual tiene la reputación de ser seguro y brinda las mismas funciones que TELNET.

**Filtrado Dinámico**

El Filtrado de paquetes Stateless sólo intenta examinar los paquetes IP independientemente, lo cual corresponde al nivel 3 del modelo OSI (Interconexión de sistemas abiertos). Sin embargo, la mayoría de las conexiones son admitidas por el protocolo TCP, el cual administra sesiones, para tener la seguridad de que todos los intercambios se lleven a cabo en forma correcta. Asimismo, muchos servicios (por ejemplo, FTP) inician una conexión en un puerto estático. Sin embargo, abren un puerto

en forma dinámica (es decir, aleatoria) para establecer una sesión entre la máquina que actúa como servidor y la máquina cliente. De esta manera, con un filtrado de paquetes stateless, es imposible prever cuáles puertos deberían autorizarse y cuáles deberían prohibirse. Para solucionar este problema, el sistema de filtrado dinámico de paquetes se basa en la inspección de las capas 3 y 4 del modelo OSI, lo que permite controlar la totalidad de las transacciones entre el cliente y el servidor. El término que se usa para denominar este proceso es "inspección stateful" o "filtrado de paquetes stateful".

Un dispositivo de firewall con "inspección stateful" puede asegurar el control de los intercambios. Esto significa que toma en cuenta el estado de paquetes previos cuando se definen reglas de filtrado. De esta manera, desde el momento en que una máquina autorizada inicia una conexión con una máquina ubicada al otro lado del firewall, todos los paquetes que pasen por esta conexión serán aceptados implícitamente por el firewall. El hecho de que el filtrado dinámico sea más efectivo que el filtrado básico de paquetes no implica que el primero protegerá el ordenador contra los hackers que se aprovechan de las vulnerabilidades de las aplicaciones. Aun así, estas vulnerabilidades representan la mayor parte de los riesgos de seguridad.

### Filtro de Aplicaciones

El filtrado de aplicaciones permite filtrar las comunicaciones de cada aplicación. El filtrado de aplicaciones opera en el nivel 7 (capa de aplicaciones) del modelo OSI, a diferencia del filtrado simple de paquetes (nivel 4). El filtrado de aplicaciones implica el conocimiento de los protocolos utilizados por cada aplicación. Como su nombre lo indica, el filtrado de aplicaciones permite filtrar las comunicaciones de cada aplicación. El filtrado de aplicaciones implica el conocimiento de las aplicaciones en la red y un gran entendimiento de la forma en que en ésta se estructuran los datos intercambiados (puertos, etc.).



Un firewall que ejecuta un filtrado de aplicaciones se denomina generalmente "pasarela de aplicaciones" o ("proxy"), ya que actúa como relé entre dos redes mediante la intervención y la realización de una evaluación completa del contenido en los paquetes intercambiados. Por lo tanto, el proxy actúa como intermediario entre los ordenadores de la red interna y la red externa, y es el que recibe los ataques. Además, el filtrado de aplicaciones permite la destrucción de los encabezados que preceden los mensajes de aplicaciones, lo cual proporciona una mayor seguridad. Este tipo de firewall es muy efectivo y, si se ejecuta correctamente, asegura una buena protección de la red. Por otra parte, el análisis detallado de los datos de la aplicación requiere una gran capacidad de procesamiento, lo que a menudo implica la ralentización de las comunicaciones, ya que cada paquete debe analizarse minuciosamente.

Virus y antivirus informático<sup>94</sup>, Además, el proxy debe interpretar una gran variedad de protocolos y conocer las vulnerabilidades relacionadas para ser efectivo. Finalmente, un sistema como este podría tener vulnerabilidades debido a que interpreta pedidos que pasan a través de sus brechas. Por lo tanto, el firewall (dinámico o no) debería disociarse del proxy para reducir los riesgos de comprometer al sistema.

### **Limitaciones del Firewall**

Por supuesto que los sistemas firewall no brindan seguridad absoluta; todo lo contrario. Los firewalls sólo ofrecen protección en tanto todas las comunicaciones salientes pasen sistemáticamente a través de éstos y estén configuradas correctamente. Los accesos a la red externa que sortean el firewall también son puntos débiles en la seguridad. Claramente, éste es el caso de las conexiones que se realizan desde la red interna mediante un módem o cualquier otro medio de conexión que evite el firewall. Asimismo, la adición de medios externos de almacenamiento a los ordenadores de sobremesa o portátiles de red interna puede dañar enormemente la política de seguridad general.

## Capítulo 6

### Documentos HTML5

Provee básicamente tres características: estructura, estilo y funcionalidad, es considerado el producto de la combinación de HTML, CSS y Javascript. El conjunto de tecnologías son altamente dependientes y actúan como una sola unidad organizada bajo la especificación de HTML que está a cargo de la estructura, CSS presenta esa estructura y su contenido en la pantalla y Javascript hace el resto.

Más allá de esta integración, la estructura sigue siendo parte esencial de un documento. La misma provee los elementos necesarios para ubicar contenido estático o dinámico, y es también una plataforma básica para aplicaciones. Con la variedad de dispositivos para acceder a Internet y la diversidad de interfaces disponibles para interactuar con la web, un aspecto básico como la estructura se vuelve parte vital del documento. Ahora la estructura debe proveer forma, organización y flexibilidad, y debe ser tan fuerte como los fundamentos de un edificio.

Para trabajar y crear sitios webs y aplicaciones con HTML5, necesitamos saber primero cómo esa estructura es construida. Crear fundamentos fuertes nos ayudará más adelante a aplicar el resto de los componentes para aprovechar completamente estas nuevas tecnologías.

Bueno dicho y hecho comencemos por definir algunos conceptos relevantes al tema de HTML5.

### *¿Qué es HTML5?*

HTML5, la última versión del Hypertext Markup Language (HTML), es la versión más radical del lenguaje a la fecha. Esta presenta muchos recursos nuevos en una variedad de áreas. Algunas de las adiciones más notables incluyen:

- Etiquetas integradas multimedia para audio y video
- Un bastidor para dibujar contenido en el navegador
- Formatos más inteligentes que le permiten hacer cosas como validación mediante el uso de un atributo requerido

Con un nuevo conjunto de etiquetas estructurales, HTML5 revisa la forma en que están estructurados los documentos HTML. Las nuevas etiquetas estructurales se enfocan en dividir un documento HTML en partes lógicas. El nombre de la etiqueta describe el tipo de contenido que se pretende que contenga. En este artículo, aprenda sobre estas nuevas etiquetas con más detalle.

### **Un poco de contexto**

Tim Berners-Lee creó el HTML original en 1989 para solucionar las deficiencias de los métodos existentes para acceder a información en Internet. Desde que se concibió, encontrar su camino en Internet era una tarea difícil. El contenido en Internet era tratado como documentos individuales, sin que hubiese métodos sencillos para navegarlos. En esencia, usted tenía que conocer la dirección del documento que estaba buscando e ingresarla manualmente. Para solucionar este problema, Berners-Lee creó dos tecnologías: Hypertext Transfer Protocol (HTTP) y HTML.

HTTP es un protocolo de servicio utilizado para entregar contenido. El comienzo de un URL en su navegador Web (suponiendo que el navegador muestre el URL completo) muy probablemente comenzará con `http://`. Esta parte del URL le dice al navegador qué tipo de protocolo usar cuando esté haciendo la solicitud al servidor Web. Cuando el servidor recibe una solicitud de documento, es probable que ese documento esté escrito o sea convertido a HTML. El documento HTML es lo que se envía de regreso al navegador que hace la solicitud.

HTML es un lenguaje de scripting que le dice al navegador Web cómo presentar el contenido. En este contenido puede haber enlaces a otros documentos, proporcionando un método fácil de usar para navegar entre documentos en Internet.

La combinación de HTTP y HTML ofrece una navegación rápida y fácil por el contenido en Internet, al permitirle simplemente hacer clic en los enlaces de texto para navegar entre documentos. Después de crear estas dos tecnologías, Berners-Lee continuó y fundó el World Wide Web Consortium (W3C). El W3C fue la fuerza guía detrás de las cuatro primeras versiones de HTML.

La intención original de Internet era servir documentos de texto simples. Los primeros navegadores todos estaban basados en texto (sin ventanas lujosas — sólo texto en una pantalla). Incluso la adición de imágenes era un gran problema cuando se introdujo al principio. Ahora, las personas hacen de todo, desde enviar mensajes de e-mail hasta ver televisión en Internet. Internet se ha convertido en mucho más que un mecanismo para transportar documentos de texto simples. Con los recursos y usos llegaron nuevos retos y problemas que el lenguaje HTML nunca fue diseñado para manejar.

El W3C intentó resolver los problemas del Internet de hoy con el estándar Extensible Hypertext Markup Language (XHTML) 2.0. Sin embargo, este estándar no fue bien recibido y fue abandonado en gran medida. En el 2004, mientras el W3C se estaba enfocando en el estándar XHTML 2.0, un grupo llamado el Web Hypertext Application Technology Working Group (WHATWG) comenzó a trabajar en el estándar HTML5, que tuvo una acogida más cálida que el estándar XHTML 2.0. El W3C abandonó el

estándar XHTML 2.0 y está trabajando ahora con WHATWG en el desarrollo del HTML5.

## Navegadores soportados

Las versiones más recientes de los navegadores más populares del mercado soportan HTML5.

*¿Por qué es importante HTML5?*

“HTML5 es el presente de la web y si no estás asimilando lo que está pasando ya eres parte de la vieja generación de desarrolladores. Eso tendría que tenerte preocupado.”

Entender HTML5 es entender que hoy nos conectamos desde teléfonos móviles, tabletas, eBooks, netbooks, computadores y otra gama de dispositivos. Es entender que se acabaron los webmasters y hoy hablamos de equipos multidisciplinarios de empresas de tecnología que cuentan con frontends, backends, sysadmins, mobile devs, community managers y arquitectos de información en los proyectos que están reinventando mercados y generando tráfico e ingresos.

Podemos hablar de todas las empresas gigantes de la web, podemos enumerar a Microsoft, Google, Apple, Adobe, Facebook, Yahoo, Mozilla y miles de proyectos tecnológicos que independientemente de sus objetivos hoy respiran HTML5, lo apoyan y tienen propuestas que los hacen competir en código en el navegador más cercano a tu pantalla. Es una de sus más importantes estrategias de posicionamiento y es una de sus más fuertes apuestas de reclutamiento. Dije además que HTML5 tiene logo de super-heroe y que venden camisetas para apoyar al movimiento.

*las nuevas etiquetas de HTML5*

HTML5 es la actualización de HTML, el lenguaje en el que es creada la web. HTML5 también es un término de marketing para agrupar las nuevas tecnologías de desarrollo de aplicaciones web: HTML5, CSS3 y nuevas capacidades de JavaScript.

La versión anterior y más usada de HTML, HTML4, carece de características necesarias para la creación de aplicaciones modernas basadas en un navegador. El uso fuerte de Javascript ha ayudado a mejorar esto, gracias a frameworks como jQuery, jQuery UI, Sproutcore, entre otros.

Flash en especial ha sido usado en reemplazo de HTML para desarrollar web apps que superaran las habilidades de un navegador: Audio, video, webcams, micrófonos, datos binarios, animaciones vectoriales, componentes de interfaz complejos, entre muchas otras cosas. Ahora HTML5 es capaz de hacer esto sin necesidad de plugins y con una gran compatibilidad entre navegadores.

### Nuevas etiquetas de HTML5

HTML4 y HTML5 son 100% compatibles entre sí. Todo el código que tienes en HTML normal seguirá funcionando sin problemas en HTML5. Para empezar a usar HTML5 lo único que tienes que hacer es colocar este DOCTYPE antes de la etiqueta `<html>`:

`<!DOCTYPE html>`

Es un DOCTYPE mucho más simplificado que XHTML (cuyas reglas siguen siendo usadas) y te permite usar todas las habilidades de HTML5 sin que nada de lo que ya tienes programado deje de funcionar.

Las principales etiquetas HTML5 nuevas no tienen una representación especial en pantalla. Todas se comportan como un `<div>` o un `<span>`. Pero cada una tiene un significado semántico superior a un simple `div` o `span`.

`<header>`

Hacer cosas como `<div id="header">` es un poco estúpido cuando el 99% de los proyectos web tienen una cabecera. `<header>` está diseñada para reemplazar la necesidad de crear divs sin significado semántico.

### `<hgroup>`

Muchos headers necesitan múltiples títulos, como un blog que tiene un título y un tagline explicando el blog. `<hgroup>` permite colocar un h1, h2 y h3 dentro del header sin afectar el SEO, permitiendo usar otro h1 en el sitio.

En el HTML actual, sólo puedes usar h1 una vez por sitio o el h1 pierde prioridad de SEO.

### `<nav>`

Igual que `<header>`, `<nav>` está diseñado para que ahí coloques la botonera de navegación principal. Puedes colocar cualquier etiqueta dentro, aunque lo recomendado es usar listas `<ul>`.

### `<section>`

Define un área de contenido única dentro del sitio. En un blog, sería la zona donde están todos los posts.

En un video de YouTube, habría un section para el video, uno para los datos del video, otro para la zona de comentarios.

### `<article>`

Define zonas únicas de contenido independiente. En el home de un blog, cada post sería un article. En un post del blog, el post y cada uno de sus comentarios sería un `<article>`.

### `<aside>`

Cualquier contenido que no esté relacionado con el objetivo primario de la página va en un aside. En un blog, obviamente el aside es la barra lateral de información. En el home de un periódico, puede ser el área de indicadores económicos.

### `<footer>`

Este es obvio. Es el pie de página y todo lo que lo compone.

Atención `<div>` no está muerto:

Estas nuevas etiquetas no significan que ya no se use <div>. Div siempre debe usarse cuando necesites una caja con objetivos de diseño gráfico o cualquier cosa que no tenga significado semántico. Sólo usa las etiquetas semánticas de HTML5 donde sean necesarias.

### *Las etiquetas nuevas importantes de HTML5*

Las etiquetas semánticas, a pesar de ser claves para posicionamiento en buscadores y buen desarrollo web, no son la razón por la que todo el mundo habla de HTML5. Video, audio y animación vectorial están en la lista de prioridades y en la boca de todas las personas que evangelizan su uso. Específicamente, las nuevas etiquetas son:

#### <video>

Inserta video sin necesidad de plugins. Es muy fácil usarla, pero cada navegador soporta codecs diferentes de video, lo que hace necesario recodificar un video en múltiples codecs. En un futuro capítulo hablamos un poco del drama que este tag está generando.

#### <audio>

Lo mismo que video, pero sin video. Puede usar múltiples formatos, en especial mp3, pero también depende del navegador.

#### <input \*>

Input ya existía como la etiqueta para insertar cajas de texto y botones. Ahora es más poderosa, con la capacidad de insertar cajas tipo “email” que se auto validan, calendarios tipo “date”, sliders, números, entre otras.

#### <canvas>

Un área de dibujo vectorial y de bit maps con Javascript. Es un API de dibujo entero para JavaScript.

#### <svg>

Una etiqueta, igual que <img>, para insertar dibujos y animaciones vectoriales al estilo de Flash.



Diferencia entre HTML Y HTML5



*Las nuevas expectativas de HTML6*

HTML5 ha hecho algunas grandes mejoras sobre HTML 4: Nos revelara nuevas etiquetas semánticas como `<nav>`, `<time>` y `<meter>`; lo que nos permite fácilmente integrar los medios de comunicación en forma de `<video>` y `<audio>` etiquetas; y dándonos un montón de increíbles API de JavaScript. Sin embargo, todavía hay un gran salto que HTML aún tiene que hacer, y ese es el salto para llegar a ser verdaderamente distribuido.

Con HTML6, usted define su propia especificación, lo que le permite marcar las cosas como desea marcarlas. En lugar de `<div class="wrapper">`, solo puedes usar `<wrapper>`.

La web se está moviendo a un ritmo más rápido que nunca, y para mantenernos al día necesitamos un marcado que se mantenga fuera de nuestro camino y nos permita hacer nuestro trabajo. Esta especificación nos permite hacer precisamente eso. Finalmente elimina las semánticas fatuas que son demasiado abstractas para que cualquiera las entienda, y brinda a los desarrolladores un lenguaje de marcado nuevo, más simple y más limpio.

Una estructura HTML bien montada soporta anotaciones de artículos utilizando párrafos, frases y palabras. Los desarrolladores web siempre están en busca de una versión dinámica y potente, que proporcione anotaciones a imágenes y vídeos. Ojalá y HTML6 ofrezca anotaciones a estos dos elementos.

## Capítulo 7

### CSS y modelos de caja

Puede que ya hayas oído hablar de CSS sin saber realmente qué es. En esta lección aprenderás más cosas sobre CSS y qué puede hacer por ti. CSS es el acrónimo de CascadingStyle Sheets (es decir, hojas de estilo en cascada).

CSS es un lenguaje de estilo que define la presentación de los documentos HTML. Por ejemplo, CSS abarca cuestiones relativas a fuentes, colores, márgenes, líneas, altura, anchura, imágenes de fondo, posicionamiento avanzado y muchos otros temas. Espera unos segundos y ya verás. Es posible usar HTML, o incluso abusar del mismo, para añadir formato a los sitios web. Sin embargo, CSS ofrece más opciones y es más preciso y sofisticado. CSS está soportado por todos los navegadores hoy día. Después de unas cuantas lecciones de este tutorial serás capaz de crear tus propias hojas de estilo usando CSS para dar a tu sitio web un aspecto nuevo y genial.

HTML se usa para estructurar el contenido; CSS se usa para formatear el contenido previamente estructurado. Vale, suena un poco técnico y

confuso. pero sigue leyendo; pronto todo tendrá sentido. Bueno en los buenos tiempos en que Madonna era una "Virgen" y un tipo llamado Tim Berners Lee inventó el World Wide Web, el lenguaje HTML sólo se usaba para añadir estructura al texto. Los autores podían marcar sus textos diciendo "esto en un título" o "esto es un párrafo", usando las etiquetas HTML `<h1>` y `<p>`, respectivamente. A medida que la Web fue ganando popularidad, los diseñadores empezaron a buscar posibilidades para añadir formato a los documentos en línea. Para satisfacer esta reclamación, los fabricantes de los navegadores (en ese momento, Netscape y Microsoft) inventaron nuevas etiquetas HTML, entre las que se encontraban, por ejemplo, `<font>`, que se diferenciaba de las etiquetas originales HTML en que definían el formato... y no la estructura. Esto también llevó a una situación en la que las etiquetas estructurales originales, por ejemplo, `<table>`, se usaban cada vez más de manera incorrecta para dar formato a las páginas en vez de para añadir estructura al texto. Muchas nuevas etiquetas que añadían formato, por ejemplo, `<blink>`, sólo las soportaban un tipo determinado de navegador. "Necesitas el navegador X para visualizar esta página" se convirtió en una declaración de descargo común en los sitios web. CSS se inventó para remediar esta situación, proporcionando a los diseñadores web con sofisticadas oportunidades de presentación soportadas por todos los navegadores. Al mismo tiempo, la separación de la presentación de los documentos del contenido de los mismos, hace que el mantenimiento del sitio sea mucho más fácil.

## *CSS y HTML*

HTML (HTML5) no describe solo los nuevos elementos HTML o el lenguaje mismo. La web demanda diseño y funcionalidad, no solo organización estructural o definición de secciones. En este nuevo paradigma, HTML se presenta junto con CSS y JavaScript como un único instrumento integrado.

La función de cada tecnología ya ha sido explicada en capítulos previos, así como los nuevos elementos HTML responsables de la estructura del

documento. Ahora es momento de analizar CSS, su relevancia dentro de esta unión estratégica y su influencia sobre la presentación de documentos HTML.

Oficialmente CSS nada tiene que ver con HTML5. CSS no es parte de la especificación y nunca lo fue. Este lenguaje es, de hecho, un complemento desarrollado para superar las limitaciones y reducir la complejidad de HTML. Al comienzo, atributos dentro de las etiquetas HTML proveían estilos esenciales para cada elemento, pero a medida que el lenguaje evolucionó, la escritura de códigos se volvió más compleja y HTML por sí mismo no pudo más satisfacer las demandas de diseñadores. En consecuencia, CSS pronto fue adoptado como la forma de separar la estructura de la presentación. Desde entonces, CSS ha crecido y ganado importancia, pero siempre desarrollado en paralelo, enfocado en las necesidades de los diseñadores y apartado del proceso de evolución de HTML.

La versión 3 de CSS sigue el mismo camino, pero esta vez con un mayor compromiso. La especificación de HTML5 fue desarrollada considerando CSS a cargo del diseño. Debido a esta consideración, la integración entre HTML y CSS es ahora vital para el desarrollo web y esta es la razón por la que cada vez que mencionamos HTML5 también estamos haciendo referencia a CSS3, aunque oficialmente se trate de dos tecnologías completamente separadas.

## *Estilos*

A pesar de que cada navegador garantiza estilos por defecto para cada uno de los elementos HTML, estos estilos no necesariamente satisfacen los requerimientos de cada diseñador. Normalmente se encuentran muy distanciados de lo que queremos para nuestros sitios webs. Diseñadores y desarrolladores a menudo deben aplicar sus propios estilos para obtener la organización y el efecto visual que realmente desean.

### ***Conceptos básicos sobre estilos***

Antes de comenzar a insertar reglas CSS en nuestro archivo de estilos y aplicar un modelo de caja, debemos revisar los conceptos básicos sobre estilos CSS.

Aplicar estilos a los elementos HTML cambia la forma en que estos son presentados en pantalla. Como explicamos anteriormente, los navegadores proveen estilos por defecto que en la mayoría de los casos no son suficientes para satisfacer las necesidades de los diseñadores. Para cambiar esto, podemos sobrescribir estos estilos con los nuestros usando diferentes técnicas.

Conceptos básicos: En este libro encontrará solo una introducción breve a los estilos CSS. Solo mencionamos las técnicas y propiedades que necesita conocer para entender los temas y códigos estudiados en próximos capítulos.

**Hágalo usted mismo:** Dentro de un archivo de texto vacío, copie cada código

HTML estudiado en los siguientes listados y abra el archivo en su navegador para comprobar su funcionamiento. Tenga en cuenta que el archivo debe tener la extensión.html para ser abierto y procesado correctamente. Estilos en línea Una de las técnicas más simples para incorporar estilos CSS a un documento HTML es la de asignar los estilos dentro de las etiquetas por medio del atributo STYLE.

El Listado muestra un documento HTML simple que contiene el elemento <p> modificado por el atributo style con el valor font-size: 20px. Este estilo cambia el tamaño por defecto del texto dentro del elemento <p>a un nuevo tamaño de 20 pixeles.

---

```
<!DOCTYPE html>
<html lang="es">
<head>
<title>Este es el título del documento</title>
</head>
```

```
<body>
<p style="font-size: 20px">Mi texto</p>
</body>
</html>
```

---

### *Estilos embebidos*

Una mejor alternativa es insertar los estilos en la cabecera del documento y luego usar referencias para afectar los elementos HTML correspondientes:

---

```
<!DOCTYPE html>
<html lang="es">
<head>
<title>Este texto es el título del documento</title>
<style>
p { font-size: 20px }
</style>
</head>
<body>
<p>Mi texto</p>
</body>
</html>
```

---

El elemento `<style>` (mostrado en el Listado) permite a los desarrolladores agrupar estilos CSS dentro del documento. En versiones previas de HTML era necesario especificar qué tipo de estilos serían insertados.

*Archivos externos*

Declarar los estilos en la cabecera del documento ahorra espacio y vuelve al código más consistente y actualizable, pero nos requiere hacer una copia de cada grupo de estilos en todos los documentos de nuestro sitio web. La solución es mover todos los estilos a un archivo externo y luego utilizar el elemento `<link>` para insertar este archivo dentro de cada documento que los necesite. Este método nos permite cambiar los estilos por completo simplemente incluyendo un archivo diferente. También nos permite modificar o adaptar nuestros documentos a cada circunstancia o dispositivo, como veremos al final del libro.

Para referenciar archivos externos se utiliza la etiqueta `<link>` y cómo utilizarla para insertar archivos con estilos CSS en nuestros documentos. Utilizando la línea `<link rel="stylesheet" href="misestilos.css">` le decimos al navegador que cargue el archivo `misestilos.css` porque contiene todos los estilos necesitados para presentar el documento en pantalla. Esta práctica fue ampliamente adoptada por diseñadores que ya están trabajando con HTML5. La etiqueta `<link>` referenciando el archivo CSS será insertada en cada uno de los documentos que requieren de esos estilos:

---

```
<!DOCTYPE html>
<html lang="es">
<head>
<title>Este texto es el título del documento</title>
<link rel="stylesheet" href="misestilos.css">
</head>
<body>
<p>Mi texto</p>
</body>
</html>
```

---



## Referencias

Almacenar todos nuestros estilos en un archivo externo e insertar este archivo dentro de cada documento que lo necesite es muy conveniente, sin embargo, no podremos hacerlo sin buenos mecanismos que nos ayuden a establecer una específica relación entre estos estilos y los elementos del documento que van a ser afectados.

Cuando hablábamos sobre cómo incluir estilos en el documento, mostramos una de las técnicas utilizadas a menudo en CSS para referenciar elementos HTML. En el Listado, el estilo para cambiar el tamaño de la letra referenciaba cada elemento `<p>` usando la palabra clave `p`. De esta manera el estilo insertado entre las etiquetas `<style>` referenciaba cada etiqueta `<p>` del documento y asignaba ese estilo particular a cada una de ellas.

Existen varios métodos para seleccionar cuáles elementos HTML serán afectados por las reglas CSS:

- *Referencia por la palabra clave del elemento*
- *Referencia por el atributo id*
- *Referencia por el atributo class*

Más tarde veremos que CSS3 es bastante flexible a este respecto e incorpora nuevas y más específicas técnicas para referenciar elementos, pero por ahora aplicaremos solo estas tres.

### *Referenciando con palabra clave*

Al declarar las reglas CSS utilizando la palabra clave del elemento afectamos cada elemento de la misma clase en el documento. Por ejemplo, la siguiente regla cambiará los estilos de todos los elementos `<p>`:

```
p {font-size: 20px}
```

Esta es la técnica presentada previamente en el Listado. Utilizando la palabra clave `p` al frente de la regla le estamos diciendo al navegador que esta regla debe ser aplicada a cada elemento `<p>` encontrado en el documento HTML. Todos los textos envueltos en etiquetas `<p>` tendrán el tamaño de 20 pixeles.

Por supuesto, lo mismo funcionará para cualquier otro elemento HTML. Si especificamos la palabra clave `span` en lugar de `p`, por ejemplo, cada texto entre etiquetas `<span>` tendrá un tamaño de 20 píxeles:

```
span {font-size: 20px}
```

Referenciando con el atributo `id` El atributo `id` es como un nombre que identifica al elemento. Esto significa que el valor de este atributo no puede ser duplicado. Este nombre debe ser único en todo el documento.

Para referenciar un elemento en particular usando el atributo `id` desde nuestro archivo CSS la regla debe ser declarada con el símbolo `#` al frente del valor que usamos para identificar el elemento:

```
#texto1 {font-size: 20px}
```

La regla en el Listado será aplicada al elemento HTML identificado con el atributo `id="texto1"`. Ahora nuestro código HTML lucirá de esta manera:

```
<!DOCTYPE html>
<html lang="es">
<head>
<title>Este texto es el título del documento</title>
<link rel="stylesheet" href="misestilos.css">
</head>
<body>
<p id="texto1">Mi texto</p>
</body>
</html>
```

### ***Referenciando con el atributo class***

La mayoría del tiempo, en lugar de utilizar el atributo `id` para propósitos de estilos es mejor utilizar `class`. Este atributo es más flexible y puede ser asignado a cada elemento HTML en el documento que comparte un diseño similar:

```
. texto1 {font-size: 20px}
```

Para trabajar con el atributo `class`, debemos declarar la regla CSS con un punto antes del nombre. La ventaja de este método es que insertar el

atributo `class` con el valor `texto1` será suficiente para asignar estos estilos a cualquier elemento que queramos:

```
<!DOCTYPE html>
<html lang="es">
<head>
<title>Este texto es el título del documento</title>
<link rel="stylesheet" href="misestilos.css">
</head>
<body>
<p class="texto1">Mi texto</p>
<p class="texto1">Mi texto</p>
<p>Mi texto</p>
</body>
</html>
```

Los elementos `<p>` en las primeras dos líneas dentro del cuerpo del código en el Listado tienen el atributo `class` con el valor `texto1`. Como dijimos previamente, la misma regla puede ser aplicada a diferentes elementos en el mismo documento. Por lo tanto, estos dos primeros elementos comparten la misma regla y ambos serán afectados por el estilo del Listado. El último elemento `<p>` conserva los estilos por defecto otorgados por el navegador.

La razón por la que debemos utilizar un punto delante del nombre de la regla es que es posible construir referencias más complejas. Por ejemplo, se puede utilizar el mismo valor para el atributo `class` en diferentes elementos pero asignar diferentes estilos para cada tipo:

```
p.texto1 {font-size: 20px}
```

Creamos una regla que referencia la clase llamada `texto1` pero solo para los elementos de tipo `<p>`. Si cualquier otro elemento tiene el mismo valor en su atributo `class` no será modificado por esta regla en particular.

*Referenciando con cualquier atributo*

Aunque los métodos de referencia estudiados anteriormente cubren un variado espectro de situaciones, a veces no son suficientes para encontrar el elemento exacto. La última versión de CSS ha incorporado nuevas formas de referenciar elementos HTML. Uno de ellas es el Selector de Atributo. Ahora podemos referenciar un elemento no solo por los atributos id y class sino también a través de cualquier otro atributo:

```
p[name] { font-size: 20px }
```

La regla en el Listado cambia solo elementos <p> que tienen un atributo llamado name. Para imitar lo que hicimos previamente con los atributos id y class, podemos también especificar el valor del atributo:

```
p[name="mitexto"] { font-size: 20px }
```

Referenciando elementos <p> que tienen un atributo name con el valor mitexto. CSS3 permite combinar “=” con otros para hacer una selección más específica:

```
p[name^="mi"] { font-size: 20px }
p[name$="mi"] { font-size: 20px }
p[name*="mi"] { font-size: 20px }
```

Si usted conoce Expresiones Regulares desde otros lenguajes como JavaScript o PHP, podrá reconocer los selectores utilizados en el Listado. En CSS3 estos selectores producen similares resultados:

- La regla con el selector ^= será asignada a todo elemento <p> que contiene un atributo name con un valor comenzado en “mi” (por ejemplo, “mitexto”, “micasa”).
- La regla con el selector \$= será asignada a todo elemento <p> que contiene un atributo name con un valor finalizado en “mi” (por ejemplo “textomi”, “casami”).
- La regla con el selector \*= será asignada a todo elemento <p> que contiene un atributo name con un valor que incluye el texto “mi” (en este

caso, el texto podría también encontrarse en el medio, como en “textomicasa”).

### ***Referenciando con pseudo clases***

CSS3 también incorpora nuevas pseudo clases que hacen la selección aún más específica.

```
<!DOCTYPE html>
<html lang="es">
<head>
<title>Este texto es el título del documento</title>
<link rel="stylesheet" href="misestilos.css">
</head>
<body>
<div id="wrapper">
<p class="mitexto1">Mi texto1</p>
<p class="mitexto2">Mi texto2</p>
<p class="mitexto3">Mi texto3</p>
<p class="mitexto4">Mi texto4</p>
</div>
</body>
</html>
```

### ***Plantilla para probar pseudo clases.***

Miremos por un momento el nuevo código HTML del Listado Contiene cuatro elementos `<p>` que, considerando la estructura HTML, son hermanos entre sí e hijos del mismo elemento `<div>`. Usando pseudo clases podemos aprovechar esta organización y referenciar un elemento específico sin importar cuánto conocemos sobre sus atributos y el valor de los mismos:

```
p:nth-child(2){
background: #999999;
}
```

La pseudo clase es agregada usando dos puntos luego de la referencia y antes del su nombre. En la regla del Listado referenciamos solo elementos `<p>`. Esta regla puede incluir otras referencias. Por ejemplo, podríamos escribirla como `.miclase:nth-child(2)` para referenciar todo elemento que es hijo de otro elemento y tiene el valor de su atributo `class` igual a `miclase`. La pseudo clase puede ser aplicada a cualquier tipo de referencia estudiada previamente.

La pseudo clase `nth-child()` nos permite encontrar un hijo específico.

### *Aplicando CSS a nuestra plantilla*

Como aprendimos más temprano en este mismo capítulo, todo elemento estructural es considerado una caja y la estructura completa es presentada como un grupo de cajas. Las cajas agrupadas constituyen lo que es llamado un Modelo de Caja.

Siguiendo con los conceptos básicos de CSS, vamos a estudiar lo que es llamado el

Modelo de Caja Tradicional. Este modelo ha sido implementado desde la primera versión de CSS y es actualmente soportado por cada navegador en el mercado, lo que lo ha convertido en un estándar para el diseño web. Todo modelo, incluso aquellos aún en fase experimental, pueden ser aplicados a la misma estructura HTML, pero esta estructura debe ser preparada para ser afectada por estos estilos de forma adecuada. Nuestros documentos HTML deberán ser adaptados al modelo de caja seleccionado.

### *Modelo de caja tradicional*

Todo comenzó con tablas. Las tablas fueron los elementos que sin intención se volvieron la herramienta ideal utilizada por desarrolladores para crear y organizar cajas de contenido en la pantalla. Este puede ser considerado el primer modelo de caja de la web. Las cajas eran creadas expandiendo celdas y combinando filas de celdas, columnas de celdas y tablas enteras, unas sobre otras o incluso anidadas. Cuando los sitios webs crecieron y se volvieron más y más complejos esta práctica comenzó a

presentar serios problemas relacionados con el tamaño y el mantenimiento del código necesario para crearlos.

Estos problemas iniciales hicieron necesario lo que ahora vemos como una práctica natural: la división entre estructura y presentación. Usando etiquetas `<div>` y estilos CSS fue posible reemplazar la función de tablas y efectivamente separar la estructura HTML de la presentación. Con elementos `<div>` y CSS podemos crear cajas en la pantalla, posicionar estas cajas a un lado o a otro y darles un tamaño, color o borde específico entre otras características. CSS provee propiedades específicas que nos permiten organizar las cajas acordes a nuestros deseos. Estas propiedades son lo suficientemente poderosas como para crear un modelo de caja que se transformó en lo que hoy conocemos como Modelo de Caja Tradicional.

## Nueva jerarquía para cabeceras

En nuestra plantilla usamos elementos `<h1>` y `<h2>` para declarar títulos y subtítulos de diferentes secciones del documento. Los estilos por defecto de estos elementos se encuentran siempre muy lejos de lo que queremos y además en HTML5 podemos reconstruir la jerarquía H varias veces en cada sección (como aprendimos en el capítulo anterior). El elemento `<h1>`, por ejemplo, será usado varias veces en el documento, no solo para el título principal de la página web como pasaba anteriormente sino también para secciones internas, por lo que tenemos que otorgarle los estilos apropiados:

```
h1 {
  font: bold 20px verdana, sans-serif;
}
h2 {
  font: bold 14px verdana, sans-serif;
}
```

La propiedad `font`, asignada a los elementos `<h1>` y `<h2>` en el Listado, nos permite declarar todos los estilos para el texto en una sola línea. Las propiedades que pueden ser declaradas usando `font` son: `font-style`, `font-variant`, `font-weight`, `font-size/line-height`, y `font-family` en este orden.

## *Creando la caja principal*

Siguiendo con el diseño de nuestra plantilla, debemos especificar un tamaño o tamaño máximo para el contenido del cuerpo. Como seguramente recuerda, en el Listado 2-25 en este mismo capítulo agregamos un elemento `<div>` a la plantilla para agrupar todas las cajas dentro del cuerpo. Este `<div>` será considerado la caja principal para la construcción de nuestro modelo de caja (este es el propósito por el que lo agregamos). De este modo, modificando el tamaño de este elemento lo hacemos al mismo tiempo para todos los demás:

```
#agrupar {
width: 960px;
margin: 15px auto;
text-align: left;
}
```

### **La cabecera**

Continuemos con el resto de los elementos estructurales. Siguiendo la etiqueta de apertura del `<div>` principal se encuentra el primer elemento estructural de HTML5:

`<header>`. Este elemento contiene el título principal de nuestra página web y estará ubicado en la parte superior de la pantalla. En nuestra plantilla, `<header>` fue identificado con el atributo `id` y el valor `cabecero`. Como ya mencionamos, cada elemento block, así como el cuerpo, por defecto tiene un valor de ancho del 100%. Esto significa que el elemento ocupará todo el espacio horizontal disponible. En el caso del cuerpo, ese espacio es el ancho total de la pantalla visible (la ventana del navegador), pero en el resto de los elementos el espacio máximo disponible estará determinado por el ancho de su elemento padre. En nuestro ejemplo, el espacio máximo disponible para los elementos dentro de la caja principal será de 960 pixeles, porque su padre es la caja principal la cual fue previamente configurada con este tamaño.



```
#cabecera {
background: #FFFBB9;
border: 1px solid #999999;
padding: 20px;
}
```

## Barra de navegación

Siguiendo al elemento `<header>` se encuentra el elemento `<nav>`, el cual tiene el propósito de proporcionar ayuda para la navegación. Los enlaces agrupados dentro de este elemento representarán el menú de nuestro sitio web. Este menú será una simple barra ubicada debajo de la cabecera. Por este motivo, del mismo modo que el elemento

`<header>`, la mayoría de los estilos que necesitamos para posicionar el elemento `<nav>` ya fueron asignados: `<nav>` es un elemento block por lo que será ubicado debajo del elemento previo, su ancho por defecto será 100% por lo que será tan ancho como su padre (el `<div>` principal), y (también por defecto) será tan alto como su contenido y los márgenes predeterminados. Por lo tanto, lo único que nos queda por hacer es mejorar su aspecto en pantalla. Esto último lo logramos agregando un fondo gris y un pequeño margen interno para separar las opciones del menú del borde del elemento:

```
#menu {
background: #CCCCCC;
padding: 5px 15px;
}
#menu li {
display: inline-block;
list-style: none;
padding: 5px;
font: bold 14px verdana, sans-serif;
}
```

## Section y aside

Los siguientes elementos estructurales en nuestro código son dos cajas ordenadas horizontalmente. El Modelo de Caja Tradicional es construido sobre estilos CSS que nos permiten especificar la posición de cada caja. Usando la propiedad float podemos posicionar estas cajas del lado izquierdo o derecho de acuerdo a nuestras necesidades. Los elementos que utilizamos en nuestra plantilla HTML para crear estas cajas son `<section>` y `<aside>`, cada uno identificado con el atributo id y los valores sección y columna respectivamente.

```
#seccion {
float: left;
width: 660px;
margin: 20px;
}
#columna {
float: left;
width: 220px;
margin: 20px 0px;
padding: 20px;
background: #CCCCCC;
}
```



