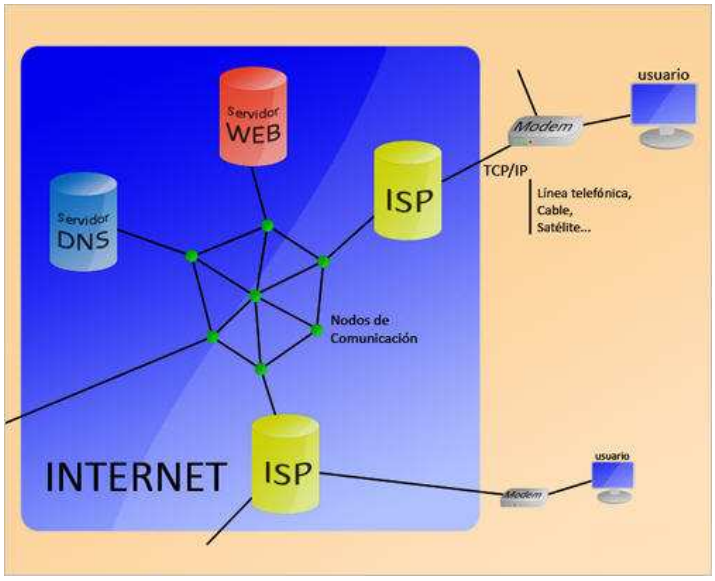
"INTERNET"

¿QUÉ ES?

Todo el mundo habla y oye hablar sobre Internet, es algo nuevo, moderno y que parece que va a cambiar nuestra forma de vivir. Pero si preguntas a la gente qué es Internet muchos no sabrán qué decirte. Vamos a intentar aclararlo con unas pocas ideas sencillas. Ya se sabe que vale más una idea clara que cien ideas confusas.

Podríamos decir que **Internet está formado por una gran cantidad de ordenadores que pueden intercambiar información entre ellos**. Es una gran red mundial de ordenadores.

Los ordenadores se pueden comunicar porque están **unidos a través de conexiones telefónicas** (aunque también pueden ser de otros tipos) y gracias a **que utilizan un lenguaje o protocolo común, el TCP/IP.**



Según el esquema que podemos ver en la imagen, un **usuario** se conecta a la red (a través de un **módem**, ya sea vía **línea telefónica, cable, satélite**, etc...). A partir de este momento el protocolo **TCP/IP** entra en juego, gracias a él puedes comunicarte con **tu Proveedor de servicios de Internet (ISP)** dándole a conocer tu dirección física.

Utilizando **TCP/IP**, el **ISP** asigna una dirección **IP** a tu **PC** y en ese momento se te da acceso a la red.

Cuando queremos acceder a una página proporcionamos un dominio que es traducido en los **Servidores DNS** y localizado. Cuando sabemos en qué **Servidor Web** se encuentra la página que queremos visitar se procede a su descarga y visualización en el navegador del **PC**.

¿QUÉ SE NECESITA PARA CONECTARSE A INTERNET?

Para conectarse a Internet se necesitan varios elementos. Hay algunos elementos que varían según el tipo de conexión que elijamos y otros que son comunes. Vamos a ver de forma genérica los distintos elementos y cuando hablemos de cada tipo de conexión los veremos de forma detallada.

En general, necesitaremos un terminal, una conexión, un módem, un proveedor de acceso a Internet y un navegador.

Terminal

El terminal es el elemento que sirve al usuario para recibir y enviar información. En el caso más común el terminal es un ordenador personal, pero también puede ser una televisión con teclado o un teléfono móvil.

Un ordenador actual de gama baja es suficiente para conectarse a Internet ya que el factor que más influye en la calidad del acceso a Internet es la velocidad de la conexión, y ésta depende del tipo de conexión que utilicemos, no del ordenador personal.

Un monitor de 19" nos permitirá trabajar con una resolución más alta (1280x1024) con lo cual veremos las imágenes más nítidamente y tendremos más sitio en la pantalla para tener varias ventanas abiertas a la vez. Un monitor de 17" tiene un campo de visión más reducido, aunque suficiente para la mayor parte de usuarios. Con un monitor de 15" la resolución recomendada es de 800x600 con locual algunas páginas web no se verán de forma completa en la pantalla y habrá que utilizar las barras de desplazamiento. El número de colores depende de los que pueda soportar la tarjeta gráfica, pero suele ser bastante alto en la mayoría de los casos.

Conexión

La comunicación entre nuestro ordenador e Internet necesita transportarse a través de algún

medio físico. La forma más básica es a través de la línea telefónica, la más utilizada en España es el ADSL y el cable.

Módem

El módem es el elemento que permite establecer la conexión física entre nuestro PC y la línea telefónica o de transmisión. El ordenador trabaja con información digital (ceros y unos) mientras que las líneas telefónicas trabajan normalmente de forma analógica (diferentes amplitudes y frecuencias de onda). El módem permite pasar de analógico a digital y viceversa, de ahí su nombre, **MO**dulador **DEM**odulador.

Según el tipo de conexión a Internet que elijamos tendremos que utilizar un tipo de módem distinto, un módem para línea telefónica básica no sirve para una línea ADSL.

Para conexiones por línea telefónica se puede utilizar un módem telefónico externo de 56 Kbps. Aunque en este caso el módem puede ser interno, si va instalado dentro del ordenador, que es la opción más común.

También se pueden utilizar módems para velocidades más altas, que son los que se utilizan en conexiones ADSL o de cable.

Los módems que incluyen Wi-Fi permiten la conexión inalámbrica entre el ordenador y el módem.

Si se necesita conectar directamente más de un ordenador al módem se pueden utilizar los módem-routers que disponen, normalmente, de cuatro salidas.

Proveedor de acceso a Internet

Una vez tenemos el terminal, módem y la conexión necesitamos que alguien nos de acceso, esta función la proporciona un proveedor de acceso a Internet (ISP).

Un ISP deberá proporcionarte todos los datos necesarios para poder crear una configuración correcta en tu PC y así poderte conectar a Internet. Aunque normalmente, los proveedores incluyen un CD de instalación que se encarga de eso, creando una configuración válida y dejando tu equipo listo para la conexión.

El ISP también asigna a nuestro ordenador un número (llamado número IP) que nos identifica dentro de Internet, así cuando solicitamos información a Internet será nuestro ordenador quien la reciba y no otro. En resumen, el ISP se encarga de gestionar la conexión entre nuestro ordenador e Internet.

Un navegador

Por último necesitaremos un programa que sea capaz de leer la información que hay en los servidores de Internet, que normalmente está escrita en el lenguaje HTML, y presentarla en pantalla formateada. También son capaces de recoger la información que introduce el usuario mediante formularios y enviarla al servidor.

Estos programas reciben el nombre de navegadores (Browsers, en inglés) y los más conocidos son el Internet Explorer de Microsoft, el Firefox de Mozilla.

Todos son gratuitos y se pueden descargar de Internet, por lo cual es fácil, además de recomendable, tener una versión actualizada. Internet Explorer viene instalado con Windows.

¿QUIÉN Y COMO SE CREA LA INFORMACIÓN EN INTERNET?

La información disponible en Internet reside en los servidores. Los **servidores o Hosts** son ordenadores conectados a la red que disponen de unos programas específicos, el software de servidor, que les permite emitir información a Internet o dicho más exactamente, los servidores permiten que se acceda a su información a través de Internet.

Los servidores de Internet pertenecen a las universidades, las instituciones públicas y a las empresas. LaS empresas de hospedaje o Hosting venden espacio a otras empresas o a particulares. Pero también hay servidores gratuitos que alojan páginas personales a cambio de publicidad.

Cada servidor proporciona diferente tipo de información, las universidades informan sobre sus planes de estudios, cursos gratuitos, logros en la investigación, etc. Las empresas dan información comercial de sus productos y servicios. Las instituciones públicas como ayuntamientos, gobiernos, etc, informan de sus servicios a los ciudadanos y las páginas personales permiten que **cualquier persona** con unos conocimientos mínimos de informática pueda poner sus ideas o conocimientos al alcance de todos.

Hoy en día, **es muy fácil publicar en Internet**, prácticamente sólo hace falta saber escribir. Aunque hay que utilizar el lenguaje HTML, hay programas que permiten escribir páginas web sin saber HMTL. Esta facilidad de creación es una de las grandezas de Internet que permite que las buenas ideas se abran paso más fácilmente que antes.

CARACTERÍSTICAS DE INTERNET

Universal.

Internet está extendido prácticamente por todo el mundo. Desde cualquier país podemos ver información generada en los demás países, enviar correo, transferir archivos, comprar, etc. Esta universalidad plantea algunos problemas legales, ya que lo que es legal en un país puede no serlo en otros. No existe una ley universal que obligue a todos los países, aunque sólo sea en aspectos relacionados con Internet.

Fácil de usar.

No es necesario saber informática para usar Internet. Podríamos decir que usar Internet es tan sencillo como pasar las hojas de un libro.

Cualquier persona debe ser capaz de navegar por un sitio web, y si no es así es porque el sitio web está mal diseñado. Esta facilidad de uso hace que Internet sea adecuada para enseñar cualquier tipo de personas desde niños a personas mayores, y se puedan hacer tareas muy diversas desde jugar hasta aprender matemáticas.

Variada.

En Internet se puede encontrar casi de todo. Por supuesto que también hay muchas cosas

inútiles, pero poco a poco irá quedando sólo lo bueno. También hay que decir que entre esta variedad hay cosas poco recomendables por lo que hay que estar atentos. Existen formas de limitar el acceso a ciertos tipos de páginas como veremos luego.

Económica.

Si piensas lo que te costaría ir a varias bibliotecas y revisar 100 libros, o visitar varias tiendas para buscar un producto y lo comparas con lo que te cuesta hacer lo mismo en Internet el ahorro de tiempo y dinero es impresionante.

Útil.

Disponer de mucha información y servicios rápidamente accesibles es, sin duda, algo útil. Hay muchos ejemplos sobre cosas que son más fáciles a través de Internet.

Libre.

El espíritu de dejar circular la información libremente es una de las razones que ha permitido el crecimiento espectacular de Internet. Si en sus comienzos los científicos que desarrollaron el soporte técnico de Internet, como el protocolo TCP/IP, no lo hubiesen puesto a disposición de la industria, hoy Internet no sería lo que es.

Hoy por hoy cualquiera puede colocar en Internet información sin censura previa, esto permite expresar libremente opiniones, y decidir libremente qué uso damos a Internet. Es algo importante que permite que las personas se sientan más libres y tengan más capacidad de reacción frente a los poderes establecidos. Pero también facilita el uso negativo de la red.

Anónima.

Podemos decir que ocultar la identidad, tanto para leer como para escribir, es bastante sencillo en Internet. Esta característica está directamente relacionada con el punto anterior, ya el

anonimato puede facilitar el uso libre de la red con todo lo que esto conlleva. Entendido de forma positiva en anonimato facilita la intimidad y la expresión de opiniones. Aunque también facilita la comisión de delitos.

Autorregulada.

¿Quién decide cómo funciona Internet? Algo que tiene tanto poder como Internet y que maneja tanto dinero no tiene un dueño personal. No hay ninguna persona o país que mande en Internet. En este sentido podemos decir que Internet se autorregula o autogestiona. La mayoría de las reglas que permiten que Internet funcione han salido de la propia Internet.

Existen unos comités internos que se encargan de regular Internet, como W3C, Internet Society, ICANN. Por ejemplo, se encargan de dictar las normas de los nombres de dominios, definir y aprobar los protocolos de comunicaciones, etc.

Un poco caótica.

Después de lo dicho en el punto anterior parece un contrasentido decir que Internet es caótica. Es caótica en el sentido que no está ordenada ni tiene unas reglas estrictas de funcionamiento que permitan asegurar que todo funciona correctamente, fundamentalmente en el aspecto del contenido.

Podemos navegar por Internet y naufragar constantemente, encontrando enlaces que no llevan a ninguna parte, páginas que dan errores, formularios que fallan, vídeos que nunca se cargan, textos descuadrados y faltas de ortografía que claman al cielo. Y esto no sólo sucede en las páginas personales, también en portales que han costado mucho dinero.

Aunque con el paso de los años se va produciendo un proceso de decantación natural, lo bueno queda arriba y lo malo se hunde en el fondo.

Insegura.

La información de Internet viaja de un lugar a otro a través de la línea telefónica y la mayoría sin encriptar. Por lo tanto es posible interceptar una comunicación y obtener la información. Esto quiere decir que se puede leer un correo o obtener el número de una tarjeta de crédito.

Es decir, si no hacemos nada la información viaja de forma insegura, pero hoy en día toda la información importante se encripta antes de enviarla por la red, y en el destino se desencripta. Además de otro tipo de medidas de seguridad. Por lo tanto las webs de sitios serios que trabajan con tarjetas de crédito, cuentas bancarias, etc, ofrecen un nivel de seguridad bastante

alto. Un sitio web que trabaja con un servidor seguro se reconoce porque aparece un pequeño candado en la barra inferior del navegador.

La inseguridad también se refiere a la existencia de virus informáticos que pueden afectar a nuestro ordenador personal, pudiendo llegar a borrar o inutilizar nuestros datos. Los virus suelen entrar a través de fallos de seguridad de los navegadores, del correo o al descargarse archivos. De la misma forma que en el caso anterior, podemos tomar medidas para evitar esta inseguridad. Actualizar los navegadores, no descargarse archivos de sitios sospechosos, no abrir correos de desconocidos, y tener instalado un programa antivirus.

¿QUÉ PODEMOS HACER EN INTERNET?

En Internet se puede hacer y encontrar prácticamente de todo. En la actualidad el factor limitante en los servicios que proporciona Internet es el ancho de banda o velocidad de

transmisión de los datos, si no hay suficiente ancho de banda, las imágenes, el sonido y el vídeo no se descargan a ritmo adecuado.

Podemos:

Buscar información.

Consultar información es lo primero que se piensa cuando se habla de utilizar Internet. Hay millones de páginas con información de todos los tipos, y en todos los idiomas.

Para ayudarnos a encontrar lo que necesitamos están los buscadores, aprender a utilizarlos correctamente puede evitarnos muchas perdidas de tiempo. A veces es sorprendente las cosas que se pueden llegar a encontrar con un buscador. Realmente vale la pena dedicar un poco de tiempo a conocerlos mejor, en este curso vamos a dedicarles mucho espacio.

La mayoría de los buscadores funcionan como motores de búsqueda, a partir de una o varias palabras clave buscan en sus bases de datos que contienen referencias a prácticamente todas las páginas de Internet. De esta clase son los buscadores Google, Alltheweb, Yahoo y MSN.

Acceso a Bases de Datos.

Se pueden acceder a multitud de bases de datos de diferentes temas.

Consultas a periódicos y revistas.

Las webs de los periódicos y revistas. Realmente ofrecen casi la misma información que las ediciones impresas y muchos de ellos empiezan a emitir versiones en PDF para que las puedas descargar y leerlas donde quieras. Incluso la mejoran añadiendo más imágenes, vídeos y gráficos animados.

Oír la radio y ver vídeos.

La transmisión de sonido, y sobre todo de vídeo, por Internet requiere que la conexión disponga del ancho de banda adecuado. Para ver y oír por Internet necesitarás tener instalado un programa que te lo permita, dos de los más utilizados son RealPlayer y Windows Media Player.

Mandar correos.

El correo electrónico o email es el servicio más utilizado de Internet junto con la Web. El email tiene muchas similitudes con el correo tradicional. Un mensaje es enviado por el remitente al destinatario. La persona que envía o remitente debe conocer la dirección del destinatario. El mensaje llega a un buzón donde permanece hasta que el destinatario lo abre y lee el correo. Éste puede eliminarlo, guardarlo o contestarlo.

El email permite escribir y enviar archivos entre dos cuentas de correo. La principal ventaja respecto al correo tradicional es su rapidez, en pocos minutos un email puede llegar a la otra punta del mundo. Otra ventaja es la comodidad, desde el ordenador lo hacemos todo, no tenemos que buscar sobres, sellos ni salir para echar la carta al buzón.

Típicamente las direcciones de correo tienen la siguiente forma **nombre@proveedor.extensión** por ejemplo, **correo@rauldiego.es** el nombre puede elegirlo el usuario al crear la cuenta o asignarlo el proveedor combinando letras del nombre y apellidos del usuario. La principal característica de una dirección de correo es que debe ser única para cada uno, no puede haber dos direcciones de correo iguales. Es mi caso, el nombre que elegí

fue **"correo"**, pues tengo un dominio que me da mi proveedor que es mi nombre **"rauldiego"** y la extensión de mi dominio es mi la de España **"es"**.

Cuando nos conectamos a Internet mediante un proveedor nos suelen asignar una o varias cuentas de correo. También podemos crear cuentas en sitios web que las ofrecen gratuitamente como **hotmail**, **yahoo**, **gmail**, etc. Estas últimas pueden ocultar la identidad del propietario de la cuenta.

Hay dos formas básicas de utilizar el correo, a) A través de un programa de correo, o b) Mediante webmail.

a) **Programa de correo**. Por ejemplo el Outlook Express de Microsoft, el Thunderbird de Mozilla, Eudora, etc. Estos son programas específicos para trabajar con el correo que tenemos que instalarnos en nuestro PC, la primera vez que se utilizan hay que configurarlos con los datos de la cuenta y servidor de correo. Por lo tanto sólo es práctico utilizarlos en el ordenador de casa y del trabajo.

Pueden manejar varias cuentas a la vez sin importar quién nos haya proporcionado la cuenta. Tienen más opciones que el webmail. En esta imagen puedes ver el aspecto general del Outlook Express:

b) **Webmail**. Esta forma de usar el correo surgió debido a la limitación que imponen los programas de correo de tener que configurarlos en cada ordenador desde donde se utilicen.

Con el webmail, desde cualquier ordenador que tenga conexión a Internet podemos leer y enviar nuestro correo sin tener que configurar nada.

Mensajería instantánea.

Este tipo de comunicación ha experimentando un aumento importante ya que posee algunas virtudes de las que el correo carece.

La mensajería instantánea tiene la característica de que cuando nos conectamos a Internet un servidor toma nota de ello y nos avisará si alguno de los usuarios de una lista que nosotros hemos dado quiere comunicarse con nosotros. En ese momento podemos decidir escribirle un correo o establecer una conversación como en un chat.

La mensajería instantánea viene a solucionar la carencia más importante del mail, no somos avisados de cuando nos llega un correo (aunque determinados programas se puede configurar para que lo hagan).

Los programas de mensajería instantánea como Microsoft MSN Messenger están integrados con el webmail y permiten ver al instante los correos que nos llegan. Para utilizar este servicio hay que instalarse un programa gratuito en el ordenador desde el que lo utilicemos.

Algunos programas de este tipo como MSN Messenger y Yahoo Messenger también permiten utilizar una webcam para ver a la persona con la que estamos hablando.

Chat.

Mediante el Chat podemos mantener una conversación con otras personas en tiempo real a través de Internet. Mientras que en el correo hay que esperar un tiempo para ver la contestación, en el chat la respuesta es instantánea.

Se puede hablar en modalidad pública, donde todos leen los mensajes de los demás, o en privado donde sólo dos personas pueden ver su conversación.

La diferencia entre el chat y la mensajería instantánea es que en el primero podemos encontrarnos con todo tipo de personas, sobretodo desconocidas, mientras que en los programas de mensajería sólo podemos hablar con nuestros contactos, es decir, con aquellas personas de las que conocemos su nombre de usuario y que han aceptado, además, admitirnos.

Telefonía IP.

La telefonía IP permite hablar por teléfono utilizando Internet como medio de transmisión de la voz, con menos calidad de recepción pero más barato, sobre todo en llamadas internacionales.

Tiene las características de una llamada telefónica convencional, es decir, debemos conocer el número de teléfono de la persona a la que llamamos y ésta debe estar en el ordenador o en el teléfono destino para recoger la llamada.

Se puede llamar desde un ordenador a un teléfono fijo o móvil, y también a otro ordenador.

Desde hace un tiempo hay un programa que está teniendo mucho éxito llamado **Skype**, permite hablar a través del ordenador a cualquier parte del mundo, con todos los que tienen instalado el programa, de forma gratuita.

Y también permite llamar a teléfonos tradicionales (móviles o fijos) pagando unas tarifas realmente bajas. Es un programa que da una excelente calidad de sonido, aún con conexiones a Internet de bajo ancho de banda, como módems telefónicos.

Videoconferencia.

La videoconferencia permite establecer una comunicación a través de Internet utilizando imágenes de vídeo y sonido en tiempo real. Se necesita disponer de un ordenador con cámara de vídeo para poder enviar imágenes, así como un micrófono. Para recibir sonido son necesarios unos altavoces y para recibir el vídeo sólo se necesita un monitor convencional.

La videoconferencia necesita transmitir gran cantidad de datos por lo que es importante disponer de una conexión con un buen ancho de banda.

News. Grupos de discusión.

Las News o grupos de discusión nacieron antes que la web alcanzase la difusión que tiene actualmente y ayudaron a compartir conocimientos entre la comunidad científica. Básicamente las News son un lugar donde los usuarios se intercambian correos, y donde se pueden aprender muchas cosas gracias al espíritu de colaboración que impera.

Los grupos de noticias o News permiten que muchas personas se comuniquen de forma escrita sobre un tema determinado. Cada participante puede enviar mensajes que todos los demás participantes pueden leer, cuando alguien responde a un mensaje, su respuesta queda "dentro" del mensaje original, lo mismo sucede con la contrarrespuesta. De esta forma cada mensaje inicial puede generar un "árbol" de respuestas que será más grande cuanto más interés susciten sus mensajes. Así cada participante ve los temas iniciales y profundiza sólo en los que le interesan.

Las News están organizadas en miles de categorías y subcategorías, y suelen encontrarse temas muy interesantes donde las personas participan con seriedad y se aprenden bastantes cosas útiles.

Para entrar en las News hay que configurarse un programa de correo dando datos como la dirección de correo y el servidor de news que nos ha proporcionado nuestro proveedor. Luego hay que elegir el tema en el que queremos participar y ya podemos enviar nuestras opiniones.

Otra alternativa es utilizar la Web mediante el servicio Google Groups (antes de que fuese comprado por Google se llamaba Deja), que nos permite buscar grupos de discusión fácilmente, incluso podemos buscar todos los mensajes en cualquier grupo de discusión en los que aparezca una determinada palabra clave. Desde este sistema, por supuesto, también podemos participar enviando mensajes.

Listas de correo web

Desde los programas de correo como Outlook se puede agrupar direcciones de correo formando una lista, de esta forma podemos enviar un mensaje a todas las personas de la lista a la vez. Partiendo de esta idea se han creado las listas de correo web que tienen unas características adicionales que las hacen más completas.

Por ejemplo, los miembros de la lista se pueden dar de alta y de baja en la lista ellos mismos desde Internet. El creador de la lista define quién está autorizado a enviar mensajes a la lista, si quiere que los mensajes sean revisados por alguien antes de ser enviados, etc.

Las listas de correo web tienen gran utilidad para mantener informados a un grupo de personas con algún interés común. Por ejemplo, los miembros de un club deportivo pueden recibir las informaciones de su club mediante un correo que los responsables sólo tienen que enviar una vez y la lista de correo se encarga de enviar un mail a cada miembro.

Foros

Otro método que está entre los más utilizados para recabar y compartir los conocimientos son los Foros. Un foro se parece mucho a un Grupo de discusión aunque mucho más simple y organizado.

Los foros están compuestos por grandes subapartados temáticos, cada uno de estos apartados trata un área de conocimiento diferente. Imagina que entramos a un foro sobre educación, podríamos encontrarnos con un subapartado que tratase sobre el nuestras asignatura.

Dentro de estos apartados encontraremos una multitud de temas empezados por los usuarios del foro y que pueden ser respondidos, completados o discutidos por cualquiera.

De esta forma se crean hilos de discusión donde la gente habla sobre temas muy específicos.

Los foros, igual que el resto de métodos que hemos visto en este apartado, cuentan con una net-etiqueta o reglas de comportamiento, donde se llama a la corrección tanto gramatical y ortográfica como en el trato con el resto de usuarios.

Descargar archivos.

Traerse información desde Internet a nuestro ordenador es una de las actividades que más éxito tienen en la red. Y no es para menos, si comparamos lo que cuesta bajarse un archivo desde Internet con lo que cuesta enviarlo por correo, por fax, etc. Además la gran cantidad de archivos puestos a disposición de la gente sería imposible de igualar por cualquier otro medio.

Para descargarse (download) archivos hay varios métodos, el más sencillo es la descarga a través de la Web, alguien coloca un archivo en el servidor de forma que el usuario sólo tiene que hacer clic y se abre una ventana para que el usuario decida en qué carpeta quiere guardar el archivo.

Clientes P2P.

A raíz de la aparición del formato mp3, que permite comprimir la música con muy poca pérdida de calidad, surgió el boom de los programas P2P como eMule y bitLord que facilitan la búsqueda y descarga de archivos.

Crear un Blog.

Un Blog o Bitácora es una página web que contiene una serie de entradas de texto o artículos que se actualizan de forma periódica. El texto más actual se coloca en primer plano para que sea lo primero que vean los visitantes al entrar en la página.

Normalmente los blogs son utilizados como diarios personales, donde sus creadores encuentran una forma de trasmitir al mundo sus ideas.

Esta forma de expresión suele adaptarse muy bien al modo en el que queremos comunicar nuestros pensamientos o conocimientos en Internet. Por eso se ha convertido en un método muy utilizado por su sencillez, en realidad es como escribir un diario, y la interfaz de estos sitios suele ser extremadamente sencilla para que cualquiera pueda publicar.

SEGURIDAD EN INTERNET

LOS VIRUS

Los virus informáticos son programas que se instalan de forma inadvertida en los ordenadores, realizan su función destructiva y pueden propagarse hacia otros ordenadores.

Las vías de propagación son diversas y han ido evolucionando a lo largo del tiempo. Hace unos años, cuando no existía Internet, se propagaban preferentemente a través de los disquetes. Luego empezaron a utilizar como vía de expansión los programas que se descargaban por Internet.

Los medios más utilizados de propagación son el email (correo por Internet) y las páginas Web. Utilizar el correo como medio de dispersión tiene varias ventajas desde el punto de vista de los virus. Es un medio muy rápido y utilizado por muchas personas, un virus puede replicarse millones de veces en pocos días de la siguiente forma.

El virus llega por correo a un ordenador y se autoenvía a todas las direcciones de correo que figuren en la Libreta de Direcciones. Al llegar a otro ordenador se vuelve a autoenviar a todas las direcciones que figuren en él, y así sucesivamente.

Los virus que utilizan las páginas Web e Internet también son capaces de reproducirse muy rápidamente puesto que una página puede ser visitada por miles de personas al día.

El ciclo de vida de un virus podría ser este, entra en nuestro ordenador, es decir, nos **infecta**, se **ejecuta** y causa, normalmente, **daños**, luego intenta copiarse en otros ordenadores, es decir **propagarse**. Cuando es **detectado** por algún programa antivirus o por el usuario es **eliminado** y muere. Vamos a ver todo esto con más detalle.

INFECCIÓN

Para que nuestro ordenador se infecte o contagie con un virus, el código del virus tiene que grabarse en nuestro ordenador, la forma más sencilla de hacer esto para un virus es cuando copiamos archivos, ya que sólo tiene que ocultarse dentro del archivo que estamos copiando.

Si sólo leemos información no podremos infectarnos, por ejemplo, si leemos el contenido de un CD o visitamos una página de la web no hay peligro de infección. Esto es la norma general, pero hay excepciones, como veremos más adelante, ya que a veces ocurre que estamos grabando cosas en nuestro ordenador sin darnos cuenta de ello.

Las **vías de infección** más comunes son:

- El correo electrónico.
- Bajarse archivos de Internet por download.
- Bajarse archivos de Internet por ftp.
- Copiar disquettes, CD, etc.
- Visitar páginas web.
- Uso de grupos de discusión.
- Uso de redes.
- Uso de redes P2P.

1- El correo electrónico

Es el método de infección más importante en la actualidad. Permite a los virus expandirse a gran velocidad ya que se envían millones de correos cada día. Algunos virus sólo se activan si abrimos los ficheros adjuntos que acompañan al mensaje.

Otros virus se activan simplemente al abrir el correo y leer el mensaje. Si tenemos activada la vista previa en nuestro programa de correo implica que se leen todos los mensajes para mostar el asunto y el remitente, por esto aunque nosotros no abramos el mensaje, el programa de correo sí lo abre y por lo tanto podemos contagiamos.

2- Bajarse archivos de Internet por download (descarga).

Hay muchas páginas web que dan la posibilidad de descargarse archivos haciendo clic en un enlace, se abre un cuadro de diálogo para preguntarnos en qué carpeta de nuestro disco duro queremos dejar el archivo y comienza la descarga. Si el archivo que descargamos está infectado puede infectar nuestro ordenador.

3- Bajarse archivos de Internet por FTP

Esta es otra forma de descargarse archivos por la red. Para ello se utilizan programas de ftp, estos programas permiten conectar con un servidor y copiar archivos del servidor a nuestro ordenador y si estamos autorizados desde nuestro ordenador al servidor.

4- Copiar información en memorias portátiles, CD, etc.

Hasta hace pocos años este era el método más utilizado por los virus para expandirse, hoy en día se copian menos archivos utilizando discos ya que es más fácil enviarlos por Internet.

5- Visitar páginas web.

Normalmente las páginas web contienen texto, gráficos, sonido, animaciones y vídeos. El navegador sólo se leen estos elementos y se visualizan en la pantalla, por lo tanto las páginas web no pueden infectarnos ya que no suelen contener programas que se ejecuten en nuestro ordenador.

Sin embargo algunas páginas web pueden grabar información en nuestro ordenador por medio de los controles ActiveX y Applets Java sin que seamos conscientes de ello. Este es un medio de infección muy peligroso y que cada vez se utiliza más, sobre todo para propagar programas espía.

6- Uso de grupos de discusión, chats.

En los grupos de discusión se intercambian mensajes y en ocasiones también archivos adjuntos, de forma similar al correo. Aunque los grupos de discusión utilizan un sistema de transmisión distinto al correo, es posible que si abrimos alguno de estos adjuntos nos podamos contagiar.

7- Uso de redes.

Podemos contagiarnos al utilizar redes globales (Internet) o redes locales.

Hasta ahora el caso más claro de infección a través de Internet ha sido el virus Sasser que contagia ordenadores por el simple hecho de conectarse a Internet, sin que el usuario visitase una página web determinada o se descargase un archivo.

Cuando utilizamos una red local estamos compartiendo recursos con los demás ordenadores de la red, si alguno de los ordenadores de la red está autorizado a escribir en nuestro disco duro podría transferirnos un virus.

8- Uso de redes P2P.

Las redes P2P (eMule, eDonkey, bitTorrent, ...) están pensadas para el intercambio de archivos y son utilizadas por millones de personas en todo el mundo, por lo tanto son el lugar ideal para colocar archivos con virus mezclados entre los archivos sanos. Hay que decir que estas redes toman medidas para evitar la presencia de virus y en cuanto detectan alguno lo eliminan o avisan a sus usuarios.

PROPAGACIÓN

La rapidez de propagación es el aspecto que determina que un virus tenga más o menos éxito. Los creadores de virus no paran de buscar nuevos métodos de propagación más rápidos y difíciles de detectar.

La propagación incluye varios aspectos como el punto de entrada en el ordenador o infección, el lugar donde esconder el archivo y la forma de activarse. Si el punto de entrada es poco común se podrán infectar pocos ordenadores. Si el archivo con el virus no se esconde bien será detectado rápidamente y no podrá propagarse. Si no se activa antes de ser detectado tampoco se expandirá mucho.

Los lugares donde se pueden esconder los virus y su forma de activarse son:

Archivos adjuntos en los correos. Al abrir el archivo adjunto el virus se activa.

Dentro del código de algunos archivos, como las macros de los documentos word o excel. Estos documentos pueden contener macros que realizan funciones adicionales en el documento, pero en el fondo una macro no es más que un programa que viaja con el documento. Al abrir el documento se ejecuta la macro y el virus se puede activar.

En la memoria del ordenador. Desde la memoria puede ejecutarse en cualquier momento y copiarse a otro archivo.

En archivos ejecutables. Los archivos ejecutables más comunes tienen extensión .exe o .com, y son los archivos que contienen programas. Estos archivos contienen código que se ejecuta al abrirlos.

En los sectores de arranque de los discos. Cada vez que se lee un disco se lee el sector de arranque del disco, es pues un buen lugar para esconder el código del virus.

En páginas web no confiables. Muchas empresas de pornografía instalan programas en nuestras computadoras para mandar publicidad o mostrar anuncios sin ningún tipo de filtro.

DAÑOS Y EFECTOS CAUSADOS

El primer fin de un virus es propagarse y el segundo fin exhibirse, mostrar que existe. Si un virus no se exhibe será más difícil de detectar.

La exhibición puede ser destructiva o festiva.

La **destructiva** puede tener varios grados, desde inutilizar algún programa o borrar un fichero concreto hasta borrar el disco duro o bloquear el sistema operativo.

La exhibición **festiva** puede consistir en mostrar algún mensaje en la pantalla o hacer que un dibujo aparezca moviéndose por la pantalla o emitir algún sonido, etc.

DETECCIÓN

¿Cómo podemos saber que tenemos un virus en nuestro ordenador?

La forma más evidente y penosa de enterarnos es como consecuencia de los daños producidos por el virus, y que acabamos de ver en el punto anterior.

Sin embargo hay algunos síntomas que nos pueden alertar de la presencia de un virus. Hay síntomas dudosos que pueden ser por un virus o por otras causas y que deben dar lugar a una investigación más profunda. Hay otros síntomas claros de que estamos infectados y que obligan a una actuación urgente.

Síntomas dudosos:

- El ordenador va muy lento.
- Disminuye la memoria disponible.
- El ordenador se apaga o bloquea frecuentemente.
- Hay programas que no funcionan o funcionan mal a partir de un momento dado.

Síntomas claros.

- Queda menos espacio libre en el disco duro sin que nosotros grabemos archivos.
- Desaparecen archivos del ordenador.
- Aparecen mensajes o gráficos extraños en la pantalla.
- Al pulsar una tecla o un acento no funciona correctamente.
- Algunos archivos cambian de nombre o de extensión.
- El lector de CD se abre y cierra solo.

La presencia de algunos de estos síntomas implica que ya se han producido daños, como en el caso de observar que han desaparecido archivos, pero siempre es bueno darse cuenta cuanto antes.

En resumen, cualquier acción extraña que no podamos asociar a ninguna otra causa puede ser causada por un virus.

La mejor forma conocida de detectar un virus para los usuarios sin conocimientos de informática es ejecutar un programa antivirus.

VIRUS (Tipos)

Los virus se pueden clasificar según diferentes criterios. Vamos a ver los más usuales.

Gusanos.

Estos virus no se copian dentro del código de otros ficheros sino que se copian ellos mismos. Los gusanos más frecuentes son los que se copian utilizando la libreta de direcciones de Microsoft Outlook. Se envían a sí mismos como ficheros adjuntos. También existen gusanos que se propagan a través de los canales de IRC. Para activarse pueden modificar el registro de Windows de forma que cada vez que se ejecute un archivo con extension .EXE el virus se activará.

Ejemplos de este tipo de virus son el virus W32/SIRCAM y el virus I_LOVE_YOU

Residentes.

Estos virus permanecen en la memoria RAM esperando a que se cumplan determinadas condiciones de activación para propagarse y causar daños. Al apagarse el ordenador desaparecen de la memoria, pero son capaces de modificar el registro de Windows para volver a colocarse en memoria cuando se enciende el ordenador.

Ejemplos de este tipo de virus son Barrotes y Viernes13. Este último está programado para borrar cualquier programa que se ejecute el dia 13, si cae en Viernes.

Troyanos.

Este tipo de virus se camufla dentro de un programa que parece inofensivo e interesante, para que el usuario lo ejecute y así llevar a cabo el fin para el que fueron programados. En ocasiones lo que pretenden es sacar al exterior información de nuestro ordenador, como podrían ser contraseñas y otros tipos de datos que pudieran ser valiosos. Por ejemplo, el troyano Crack2000 se distribuye junto con un programa que dice llevar los números de serie de aplicaciones comerciales, una vez instalado hace que se envie por FTP la información grabada en el disco duro.

Macros.

Estos virus están dentro del código de las macros de programas como Excel, Word, CorelDraw,… Por ejemplo el virus Melissa es una macro de Word97.

Ejecutables.

Gran parte de los virus forman parte del código de ficheros ejecutables de extensión .EXE y .COM. Podríamos decir que es el tipo de virus más común. Estos virus se ejecutan cuando lo hace el fichero en el que se encuentran y utilizan diversos medios para propagarse. Los virus incluidos en ficheros ejecutables no son un tipo puro de virus sino que pueden tener además alguna de las características de otros tipos de virus. Por ejemplo hay virus ejecutables que se propagan por el correo como los virus tipo gusano.

MALWARE

Todos estos sistemas de propagación que hemos visto no se aprovechan únicamente para infectarnos con Virus, si no que también se utilizan para instalar en nuestros ordenadores programas que maliciosamente interfieren con la información que envíamos o poseemos.

Este tipo de programas se llama Malware. El Malware está diseñado para insertar y distribuir virus, troyanos, o pequeños programas que recogerán información sobre nuestro ordenador y lo utilizará con malas intenciones.

El Malware, también, suele ir incrustado o añadido en programas gratuitos de dudosa procedencia que podemos encontrar por Internet. Ten cuidado con ellos porque pueden llegar a ser igual de desastrosos que los virus.

El Malware también se dedica a instalar **Spyware** en nuestro ordenador.

SPYWARE

Un programa espía o Spyware recopila información sobre nosotros y lo envía normalmente a

empresas de publicidad. De esta forma podemos empezar a recibir SPAM sin haberlo pedido expresamente.

Si a pesar de todo el Spyware se instala en tu ordenador, existen herramientas anti-spyware (como Spybot) que recorren tu disco en busca de programas instalados que pudieran ser maliciosos (de ahí también el término Malware) y peligrosos para tu privacidad.

SPAM

SPAM es la palabra que se utiliza para calificar el correo no solicitado con fines comerciales o publicitarios enviado por Internet.

Los usuarios que los reciben pagan por el envío de su propio bolsillo, el Spam es una publicidad cuyo coste recae en quien la recibe aunque no quiera hacerlo. Cualquiera que tenga un servicio de acceso a Internet que pague por tiempo o por tráfico, lee o recibe mensajes, como si dijéramos, con el contador en marcha, los que tienen tarifas planas funcionan peor.

Todas las conexiones van más lentas debido a las ingentes cantidades de tráfico que genera el Spam, leer los mensajes Spam incrementa su factura de teléfono, le ocupa tiempo, espacio en su buzón y le puede hacer perder información que se quiere recibir.

Por lo tanto:

- Sólo hay que dar la dirección E-mail a amigos y conocidos.
- No publicar la dirección E-mail en las News o en páginas Web.
- No rellenar formularios en los que se soliciten datos personales.
- Nunca hay que contestar a un mensaje de Spam ya que en muchos casos la dirección del remitente será falsa y devuelven el mensaje y si no es falsa sirve a la empresa de publicidad para saber que la dirección E-mail es correcta.

PHISING

Por último veremos un método malicioso que prentende hacerse con la información de nuestras cuentas bancarias: el Phishing.

El Phishing se está poniendo muy de moda últimamente, millones de usuarios reciben a diario correos de entidades bancarias pidiendo que se proporcionen claves o números de cuenta a los usuarios para realizar una serie de comprobaciones.

En ningún momento tu entidad bancaria, tu sitio de micropagos (PayPal) o cualquier empresa te requerirá datos sobre tus cuentas bancarias por e-mail.

Lo que reproducen estos correos son avisos de ciertas entidades imitando su diseño. Normalmente aparecen enlaces a páginas que a primera vista parecen ser de tu propio banco, pero si miramos con más atención nos damos cuenta de que son servidores que no tienen nada que ver con él.

Estos enlaces dirigen en realidad a páginas creadas por personas malintencionadas que pretenden que les proporcionemos la información suficiente como para vaciarnos la cuenta corriente.

PRECAUCIONES

- No hay que abrir **correos de desconocidos** o que nos merezcan poca confianza.

- No abrir **archivos adjuntos** si no se tiene la certeza de su contenido incluso si proviene de una dirección "amiga".

- También es conveniente fijarse en el **texto del Asunto**, si es un texto sin un significado claro puede ser un síntoma de que el correo contiene un virus ya que algunos virus generan el asunto juntando varias palabras al azar.

- Desactivar la opción de **"Vista previa"** de algunos programas de correo, como por ejemplo el Outlook Express. Así evitamos que siempre se lea el mensaje para poder mostrar la Vista Previa.

- Hay que tener mucho cuidado con los **archivos y programas que nos bajamos de Internet**, especialmente de sitios sospechosos.

- **Utilizar un Antivirus**. Los programas antivirus pueden trabajar de dos formas básicas. De forma permanente y bajo petición.

    - De forma permanente quiere decir que el antivirus se instala de forma residente en memoria y busca virus en todos los archivos que se abren o descargan de Internet. Es la forma más segura de protegerse de los virus. Tiene el pequeño inconveniente que consume memoria RAM y en algunas ocasiones puede interferir el funcionamiento de algunos programas.
    - De forma puntual o bajo petición, podemos tener el antivirus desactivado y activarlo sólo cuando consideremos que hay peligro de contagio, por ejemplo cuando descargamos archivos de Internet, copiamos un disquete o instalamos un programa nuevo. **Es conveniente tener activado el antivirus de forma permanente.**

UTILIZACIÓN DE UN CORTAFUEGOS

Cortafuegos

Un **cortafuegos o firewal** (en Inglés) es un sistema hardware y/o software que permite controlar quién entra y quién sale del ordenador. Es como un filtro que impide que se puedan colar intrusos en nuestro ordenador.

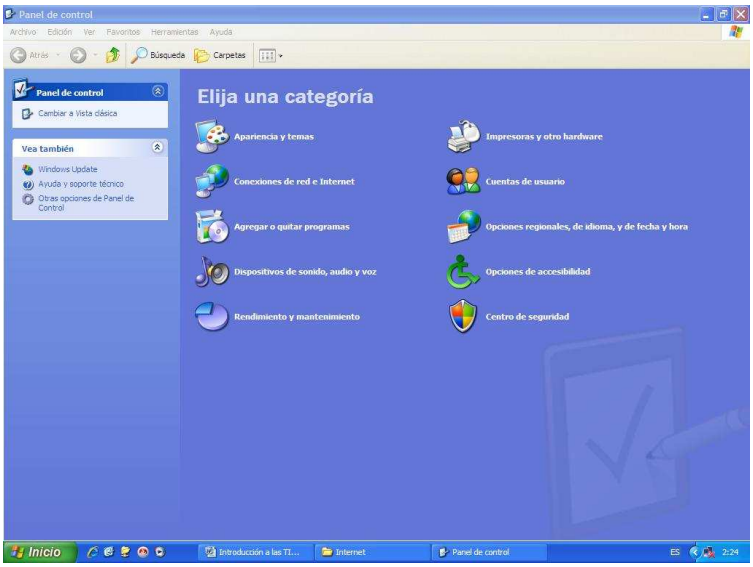
Hoy en día existe una nueva amenaza, es la intrusión en los ordenadores conectados a redes sin que el usuario se descargue nada ni visite ninguna web, simplemente con estar conectado es suficiente para que alguien pueda entrar e instalar programas espía (spyware) o programas fraudes (phishing) o llegar a controlar totalmente el ordenador.

Todo esto puede estar sucediendo en tu ordenador sin que te enteres, hasta hace poco, contra estos ataques, los programas antivirus convencionales no solían protegernos, ya que hace falta un cortafuegos. Actualmente, los cortafuegos suelen venir incluidos con la mayoría de antivirus de pago y son un complemento más del programa, aunque a veces no suelen estar incluidos en las versiones básicas. Las últimas versiones de Windows XP (a partir del ServicePack2) también incluyen uno.

Para configurar un cortafuegos hay que definir unas reglas que determinan quien puede y quien no puede acceder al ordenador.

El centro de seguridad de Windows es el encargado de supervisar el estado del quipo en cuanto a protección se refiere.

Puedes acceder a él haciendo clic en **Inicio** → **Panel de control** y seleccionando **Centro de seguridad.**



En él hay tres puntos importantes: el **Firewall o cortafuegos**, las **Actualizaciones automáticas** y la **Protección antivirus**.

Haciendo clic en **Firewall de Windows** podrás ver un cuadro de diálogo parecido al que ves en la imagen a la derecha. (Selecciona la pestaña **Excepciones** para la configuración avanzada).

Desde la pestaña **Excepciones** podemos elegir qué programas queremos que tengan acceso a Internet. De esta forma sólo aquellos que nosotros queramos podrán comunicarse con el exterior.

Ahora imagina que se instala un troyano en tu computador. Cuando se ejecute intentará ponerse en contacto con el exterior para enviar información.

Si el troyano no está en esta lista no será capaz de acceder a la red.

Haciendo clic en el enlace **Actualizaciones automáticas** (en la ventana del Centro de seguridad).

Desde aquí podemos controlar cómo se producirá el flujo de actualizaciones en nuestro ordenador.

Una de las causas de la infección son los fallos o agujeros en los programas que utilizamos, entre ellos el sistema operativo (Windows), los programas de navegación (Internet Explorer) o de reproducción de archivos (Windows Media Player).

Ambos productos pertenecen a Microsoft, por lo que se ha creado está característica.

A medida que se van descubriendo nuevos puntos flacos en los programas, se van liberando parches o soluciones.

Finalmente, si observas el Centro de seguridad verás que hay una sección dedicada al **Antivirus**.

Windows no puede acceder a la configuración del programa antivirus que tengas instalado en tu PC, pero sí puede avisarte sobre su estado.

Si en algún momento tu antivirus se queda desactualizado, es decir, su base de datos sobre virus es demasiado antigua, Windows te avisará a través del Centro de seguridad.

Si no quieres instalarte un programa antivirus, y tampoco quieres que Windows te avise de que tu equipo corre peligro puedes desactivar estos avisos seleccionando **Protección antivirus** y haciendo clic en el botón **Recomendaciones**.

Se abrirá el cuadro de diálogo que ves a tu derecha, marca la casilla **Tengo un programa antivirus que yo supervisaré.**

De todas formas, aunque tengas instalado un antivirus, es posible que Windows no lo detecte. Sigue estos mismos pasos para evitar el aviso continuado de que tu equipo está en riesgo.