# Conceptos vinculados a la tecnología

**SPAM:**

El SPAM es un problema para los usuarios de Internet que reciben diariamente en sus buzones docenas de e-mails no deseados en los que se les oferta variados artículos para aumentar su potencia sexual o conseguir una tupida melena. También es un problema muy serio para las empresas que ven cómo sus correos publicitarios o comerciales por algún misterioso motivo son catalogados como SPAM y no llegan a sus clientes.

Lo primero que debe conocer son los **dos motivos** principales por los que sus correos pueden ser catalogados como SPAM:

1. Los destinatarios de sus correos no **deseaban recibirlos** o **no son capaces de visualizarlos** correctamente y realizan una denuncia de SPAM en las listas **RBL** (listas negras públicas internacionales).

2. Sus correos son detectados automáticamente como SPAM por un **filtro Bayesiano**.

Consejos muy concretos y prácticos, que ayudan a optimizar el ratio de recepción de campañas de Marketing:

**1. Filtre su base de datos de e-mails para evitar envíos innecesarios.**

- **Elimine e-mails incorrectos** de su base de datos. Los correos del tipo aa@aa.es son fácilmente descartables.

- Ofrezca un servicio para que sus clientes puedan **actualizar sus correos**: Más del 30% de sus clientes podrán cambiar de correo a lo largo de un año.

- Utilice **servicios de *list hygiene***: Más del uno por ciento de sus correos serán direcciones mal formadas del tipo johngmail.com que claramente deberían ser john@gmail.com. Las aplicaciones de list hygiene son capaces de corregir este tipo de errores de sus bases de datos.

- **Elimine de su base de datos direcciones de correo "*Spam flag*"**: Se trata de direcciones de correo que se han añadido de manera malintencionada y que pueden hacer que su empresa se autodenuncie en listas negras. Por ejemplo: abuse@somedomain.

**2. Tenga presente la siguiente guía de Buenas prácticas para obtener el permiso de las personas que recibirán sus e-mails.**

- Realice el **sistema de suscripciones más conservador** que pueda permitirse: Antes de incluir una dirección de correo en su base de datos, la mayoría de las empresas envían a sus suscriptores un correo de confirmación en el que se solicita que confirmen su interés en recibir información comercial por correo.

- Conserve **la dirección IP de sus suscriptores**: Le permitirá cubrirse las espaldas en el caso de que se vea en la necesidad de conversar con ISPs y Listas negras.
- Evite comprar listas de e-mails, y si lo hace, investigue la fuente de estas listas. Puede recurrir a un *trustworthy list broker* para que le asesore en la adquisición de una lista de calidad.
- Permita que sus clientes puedan **desuscribirse de manera clara, sencilla y rápida**.

**3. Elija el ISP de su servidor de correo cuidadosamente.**

Si su ISP ha sido denunciado a una blacklist, los correos que envía a través de sus servidores serán catalogados como SPAM. Puede apuntarse a la siguiente lista de discusión sobre SPAM http://peach.ease.lsoft.com/archives/spam-l.html donde podrá buscar ISP de confianza.

**4. Cuide minuciosamente el contenido del Asunto y cuerpo de sus correos para evitar los filtros anti-spam por contenido o filtros Bayesianos.**

Los filtros Bayesianos aunque representan la última técnica en la lucha contra el SPAM se basan en un método estadístico descubierto en el siglo XVIII, por el clérigo y matemático Thomas Bayes, (1701-1761). La estadística bayesiana es una herramienta muy eficaz para poder calcular la probabilidad de que ocurra un suceso determinado, en nuestro caso que un e-mail sea SPAM. Para realizar este cálculo estadístico nos basamos en la experiencia de lo ocurrido anteriormente en casos semejantes.

Para evitar que nuestros e-mails sean catalogados como SPAM por un filtro Bayesiano es importante que conozcamos cómo funcionan: Cuando un ISP recibe un email y una persona determina **manualmente** que se trata de un caso de spam, se observa la **frecuencia** relativa de cada una de las palabras del mensaje, se calcula su **probabilidad** de ocurrencia y se actualiza el filtro Bayesiano con esta información. También se hace exactamente lo mismo con los mensajes que se reciben y son considerados como no spam.

Cuando ya hemos entrenado a nuestro filtro Bayesiano con muchas palabras asociadas a la práctica de spam y no-spam, podemos pedirle que calcule de manera automática la probabilidad de que cada e-mail que se reciba sea o no sea spam en función de las palabras que contiene, por ejemplo *"viagra" ó "gratis", "enlarge".* Así se calcula la probabilidad de que el mensaje sea spam. A esta cifra se le llama *"spamicidad" y* cuando supera un umbral (por ejemplo el 90%), se puede clasificar de manera segura como spam.

Una vez entrenado, un filtro Bayesiano ofrece muy pocos *falsos positivos,* ya que a diferencia de otros filtros, ataca la esencia del problema del spam: el contenido del mensaje. Recuerde que el método bayesiano es multilingüe e internacional, un filtro anti-spam bayesiano, al ser adaptable, puede utilizarse con cualquier idioma.

Por tanto, para evitar los filtros Bayesianos debe prestar especial atención al contenido y redacción de sus e-mails:

- Evite utilizar un estilo demasiado **comercial** en la redacción de sus contenidos.
- Evita las expresiones y palabras demasiado **agresivas** como "FREE", "*GRATIS*", "*COMPRE AHORA*" o "*DESCUENTOS*".
- No escriba **nunca en mayúsculas** en el Subject.
- Evite el **uso excesivo de signos de admiración o símbolos** como $$.
- Evite la utilización de la frase **"haga click aquí ".**
- Evite las **frases redundantes** y las instrucciones **poco concisas**.

Además, las más avanzadas soluciones en materia anti-spam incluyen un motor de filtro bayesiano de segunda generación, lo que supone no sólo un simple análisis de texto, sino también un amplio exámen de la forma y los atributos de los archivos adjuntos.

Si tiene curiosidad por ver cómo funcionan los filtros bayesianos, puede descargarse el programa gratuito anti SPAM K9 desde esta dirección.

**5. Cuide el código HTML de sus e-mails:**

- Evite las imágenes de fondo, en muchos webmails no se visualizarán.
- No ponga texto editable sobre las imágenes de fondo, pues al desaparecer la imagen perderán su contexto.
- Todas las imágenes deben tener la etiqueta "ALT" y "TITLE" con su correspondiente texto descriptivo.
- No utilice hojas de estilo CSS externas, ni declare los estilos en la cabecera pues algunos webmails los eliminan.
- Aplique los estilos CSS directamente sobre los tags (style="…").
- Utilice tablas para la maquetación de sus contenidos.
- Evite siempre incluir controles ActiveX
- No utilice imágenes animadas ni flash.
- Incluya siempre el charset para la definición de los caracteres en el idioma correspondiente.

**6. Configure correctamente su infraestructura de envío de e-mails:**

- Mantenga activada la **resolución inversa de DNS**: Muchos filtros de correo utilizan la resolución inversa para asegurarse que la compañía que se supone está enviando los e-mails es realmente el emisor. En el caso de que no esté activa, sus correos no se enviarán.
- Compruebe si mantiene **Relays abiertos** en su servidor de correo y **ciérrelos**: Los Spammers a menudo buscan relays abiertos para enviar sus correos a través de los servidores de correo de otras compañías.
- No haga **relay entre servidores** antes de enviar los correos: Los correos de algunas empresas suelen viajar entre varios servidores internos antes de entregarlos al destinatario final; ésto podría ser irrelevante si no fuera porque el relay entre servidores es una práctica habitual entre los Spammers para intentar ocultar la procedencia de sus correos. Tenga en cuenta que cuanto menos relay haga, menos dudas habrá sobre la procedencia de sus correos.
- Utilice un **formMail seguro** en su página web: Un agujero de seguridad en su formulario de envio de correos puede ser una puerta abierta para que los Spammers envíen información desde su servidor de correo.

**7. Monitorice constantemente su sistema para saber si está ocurriendo un problema. Hay varias formas de saber cuándo hay un problema en la entrega de los correos:**

- Monitorice los **ratios de entrega** por dominio: De esta manera puede comprobar por ejemplo si hay una caida en los ratios de entrega de correos de GMail.
- Monitorice sus campañas de e-mails **antes de comenzarlas**: Antes de lanzar una campaña es importante asegurarse que nuestros correos serán aceptados por los principales ISP (en la práctica los 15 ISPs principales representan el 60% del mercado). Existen empresas de seguridad que ofrecen servicios de chequeo automático de e-mails para saber si sus campañas pasarán los filtros antispam de los principales ISPs.
- Monitorice las **blacklists**: Compruebe si su servidor de correo está dentro de alguna lista negra. Algunos sistemas de seguridad ofrecen un servicio de Blacklist Alert que le alerta si su servidor de correo se encuentra en más de 300 blacklists.

**8. Mantenga buenas relaciones con los ISPs.**

Siempre es de ayuda saber a quién dirigirse cuando hay un problema, pero recuerde que para mantener una buena relación es importante dedicarle mucho tiempo y recursos.

**9. Y por supuesto, no haga SPAM.**

El envío masivo e indiscriminado de e-mailings a personas que no los han solicitado, no le harán incrementar sus ventas. Por el contrario dañara la imagen de su empresa y tarde o temprano acabará originándole serios problemas.

Espero que con la ayuda de estos consejos sus campañas de e-marketing acaben llegando siempre a buen puerto.

## SEO:

Significa  Search Engine Optimization, que se puede traducir como Optimización motores de búsqueda. Es la ingeniería desarrollada para mejorar la ubicación de un sitio web en la respuesta de los buscadores.

## Landing Page:

En la mercadotecnia en Internet, se denomina **página de aterrizaje** (del inglés *landing pages*) a una página web a la que una persona llega, después de haber pulsado en el enlace de algún *banner* o anuncio de texto situado en otra página web o portal de Internet. En la mayoría de los casos esta página web es una extensión del anuncio de promoción, donde se explica más detalladamente la oferta del producto o servicio que se está promocionando a través de una carta de ventas.

También esta página suele estar optimizada para unas determinadas palabras clave, con el objetivo de conseguir que los buscadores la indexen correctamente y la muestren cuando el prospecto realiza una búsqueda introduciendo esas palabras clave. Así se pueden tener diferentes *páginas de aterrizaje* que promocionan el mismo producto, pero optimizadas para diferentes palabras clave, lo que maximiza las posibilidades de conseguir que más potenciales clientes lleguen hasta la página de oferta.

Este tipo de páginas también pueden ser llamadas de otras formas como: páginas de salto (*jump pages* en inglés). Algunas personas suelen llamarla *splash pages*, pero este último término identifica, en realidad, a las páginas de inicio o *intro*, habitualmente realizadas en Flash en forma llamativa que funcionan como *peaje* electrónico antes de la carga total de contenido o con fines decorativos, persuasivos, etc. Recientes estudios de autores como Jakob Nielsen descalifican el uso de *splash pages*, ya que los usuarios tienden a sortearlas o abandonar el sitio, si la presentación es deficiente comunicacionalmente, o demasiado extensa para su carga y visualización.

## Webmaster

Es la persona responsable de mantenimiento o programación de un sitio web. La definición específica de este cargo puede variar según el ámbito en el que se presente a la persona: en ciertos casos es el responsable de los contenidos del sitio,[1] mientras que en otros es el encargado de la operatibilidad, programación y mantenimiento de la disponibilidad de un sitio web sin que necesariamente intervenga en la creación de contenidos.

## RSS

**RSS** son las siglas de **Really Simple Syndication**, un formato XML para sindicar o compartir contenido en la web. Se utiliza para difundir información actualizada frecuentemente a usuarios que se han suscrito a la fuente de contenidos. El formato permite distribuir contenidos sin necesidad de un navegador, utilizando un software diseñado para leer estos contenidos RSS (agregador). A pesar de eso, es posible utilizar el mismo navegador para ver los contenidos RSS. Las últimas versiones de los principales navegadores permiten leer los RSS sin necesidad de software adicional. RSS es parte de la familia de los formatos XML desarrollado específicamente para todo tipo de sitios que se actualicen con frecuencia y por medio del cual se puede compartir la información y usarla en otros sitios web o programas. A esto se le conoce como redifusión web o *sindicación web*(una traducción incorrecta, pero de uso muy común).

## Podcast

El ***podcasting*** consiste en la distribución de archivos multimedia (normalmente audio o video, que puede incluir texto como subtítulos y notas) mediante un sistema de redifusión (RSS) que permita suscribirse y usar un programa que lo descarga para que el usuario lo escuche en el momento que quiera. No es necesario estar suscrito para descargarlos.

## Streaming

El ***streaming*** es la distribución de multimedia a través de una red de computadoras de manera que el usuario consume el producto al mismo tiempo que se descarga. La palabra *streaming* se refiere a que se trata de una corriente continua (sin interrupción). Este tipo de tecnología funciona mediante un búfer de datos que va almacenando lo que se va descargando para luego mostrarse al usuario. Esto se contrapone al mecanismo de descarga de archivos, que requiere que el usuario descargue los archivos por completo para poder acceder a ellos.

El término se aplica habitualmente a la difusión de audio o video. El streaming requiere una conexión por lo menos de igual ancho de banda que la tasa de transmisión del servicio. El streaming de video se popularizó a fines de la década de 2000, cuando el ancho de banda se hizo lo suficientemente barato para gran parte de la población.

Para poder proporcionar un acceso claro, convincente, continuo y sin interrupciones ni cambios, el *streaming* se apoya en las siguientes tecnologías:

### Códecs

Son archivos residentes en el ordenador que permiten a uno o varios programas descifrar o interpretar el contenido de un determinado tipo de archivo multimedia.

### Protocolos Ligeros

UDP y RTSP (los protocolos empleados por algunas tecnologías de "*streaming*") hacen que las entregas de paquetes de datos desde el servidor a quien reproduce el archivo se hagan con una velocidad mucho mayor que la que se obtiene por TCP y HTTP. Esta eficiencia es alcanzada por una modalidad que favorece el flujo continuo de paquetes de datos. Cuando TCP y HTTP sufren un error de transmisión, siguen intentando transmitir los paquetes de datos perdidos hasta conseguir una confirmación de que la información llegó en su totalidad. Sin embargo, UDP continúa mandando los datos sin tomar en cuenta interrupciones, ya que en una aplicación multimedia estas pérdidas son casi imperceptibles.

## Precarga o Buffer

La entrega de datos desde el servidor a quien ve la página pueden estar sujetas a demoras conocidas como lag, (retraso, en inglés) un fenómeno ocasionado cuando los datos escasean (debido a interrupciones en la conexión o sobrecarga en el ancho de banda). Por tanto, los reproductores multimedia precargan, o almacenan en el *buffer*, que es una especie de memoria, los datos que van recibiendo para así disponer de una reserva de datos, con el objeto de evitar que la reproducción se detenga. Esto es similar a lo que ocurre en un reproductor de CD portátil, que evita los saltos bruscos y los silencios ocasionados por interrupciones en la lectura debidos a vibraciones o traqueteos, almacenando los datos, antes de que el usuario tenga acceso a ellos.

## Red de Acceso de Contenido

Si un determinado contenido comienza a atraer una cantidad de usuarios mayor a su capacidad de ancho de banda, estos usuarios sufrirán cortes o lag. Finalmente, se llega a un punto en que la calidad del *stream* es pésima. Ofreciendo soluciones, surgen empresas y organizaciones que se encargan de proveer ancho de banda exclusivamente para *streaming*, y de apoyar y desarrollar estos servicios.

# Multicast

**Multidifusión** es el envío de la información en una red a múltiples destinos simultáneamente.

Antes del envío de la información, deben establecerse una serie de parámetros. Para poder recibirla, es necesario establecer lo que se denomina "grupo multicast". Ese grupo multicast tiene asociado una dirección de internet. La versión actual del protocolo de internet, conocida como IPv4, reserva las direcciones de tipo D para la multidifusión.

## Peer tu peer

Una **red Peer-to-Peer** o **red de pares** o **red entre iguales** o **red entre pares** o **red punto a punto** (**P2P**, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

Las redes *peer-to-peer* aprovechan, administran y optimizan el uso del ancho de banda de los demás usuarios de la red por medio de la conectividad entre los mismos, y obtienen así más rendimiento en las conexiones y transferencias que con algunos métodos centralizados convencionales, donde una cantidad relativamente pequeña de servidores provee el total del ancho de banda y recursos compartidos para un servicio o aplicación.

Dichas redes son útiles para diversos propósitos. A menudo se usan para compartir ficheros de cualquier tipo (por ejemplo, audio, vídeo o software). Este tipo de red también suele usarse en telefonía VoIP para hacer más eficiente la transmisión de datos en tiempo real.

## Video on demand

La **televisión a la carta** o **vídeo bajo demanda**, del inglés **video on demand (VoD)** es un sistema de televisión que permite al usuario el acceso a contenidos multimedia de forma personalizada ofreciéndole, de este modo, la posibilidad de solicitar y visualizar una película o programa concreto en el momento exacto que el telespectador lo desee. Existe, por tanto, la posibilidad de visualización en tiempo real o bien descargándolo en un dispositivo como puede ser un ordenador, una grabadora de vídeo digital (también llamada grabadora de vídeo personal) o un reproductor portátil para verlo en cualquier momento.

El sistema contiene las funciones básicas de video, como la opción de detener el programa o reanudarlo a voluntad del mismo cliente, llevarlo hacia delante y hacia atrás, ponerlo a cámara lenta o en pausa; son los llamados modos trampa. Además**VoD** permite al usuario disponer del programa deseado sin depender de horarios fijos de programación. El espectador dispone de una amplia oferta de programas para visualizar o realizar un pago por ciertos programas como en el caso de pago por visión. El cliente está conectado a un servidor de Video on Demand que dispone de un sistema alternativo a los tradicionales alquileres de películas.

En los sistemas de streaming basados en disco tenemos la necesidad de un procesamiento adicional, ya que los archivos separados de avance rápido y retroceso deben ser almacenados en unidades de disco duro. En cambio, los sistemas basados en memoria pueden ejecutar estos sistemas directamente desde la RAM ya que no necesita almacenamiento adicional.

Tenemos dos posibles maneras de distribución de VoD; el primer caso es a través de LAN, podemos realizar una distribución mucho más rápida a los usuarios. En cambio, si lo hacemos a través de WAN, la respuesta es más lenta pero el alcance será mucho más amplio.

Los servicios de descarga VoD son posibles en casas con conexión vía cable (óptico o coaxial) o bien ADSL. VoD utiliza protocolos en tiempo real, como por ejemplo RTP (Real Time Protocol)

sobre UDP (User Datagram Protocol) con el protocolo de control RTCP (Real Time Control Protocol). Un buen complemento sería un protocolo de reserva de recursos como el RSVP (ReSerVation Protocol).

## Publicidad viral

El **marketing viral** es un término empleado para referirse a las técnicas de marketing que intentan explotar redes sociales y otros medios electrónicos para producir incrementos exponenciales en "renombre de marca" (*Brand Awareness*), mediante procesos de autorreplicación viral análogos a la expansión de un virus informático. Se suele basar en el boca a boca mediante medios electrónicos; usa el efecto de "red social" creado por Internet y los modernos servicios de telefonía móvil para llegar a una gran cantidad de personas rápidamente.

También se usa el término *marketing viral* para describir campañas de marketing encubierto basadas en Internet, incluyendo el uso de blogs, de sitios aparentemente amateurs, y de otras formas de *astroturfing* diseñadas para crear el boca a boca para un nuevo producto o servicio. Frecuentemente, el objetivo de las campañas de marketing viral es generar cobertura mediática mediante historias "inusuales", por un valor muy superior al presupuesto para publicidad de la compañía anunciante.

El término *publicidad viral* se refiere a la idea que la gente se pasará y compartirá contenidos divertidos e interesantes. Esta técnica a menudo está patrocinada por una marca, que busca generar conocimiento de un producto o servicio. Los anuncios virales toman a menudo la forma de divertidos videoclips o juegos Flash interactivos, imágenes, e incluso textos.

La popularidad creciente del marketing viral se debe a la facilidad de ejecución de la campaña, su coste relativamente bajo, (comparado con campañas de correo directo), buen "targeting", y una tasa de respuesta alta y elevada. La principal ventaja de esta forma de marketing consiste en su capacidad de conseguir una gran cantidad de posibles clientes interesados, a un bajo costo.

## Malware

**Malware** (del inglés ***mal****icious soft****ware***), también llamado **badware**, **código maligno**, **software malicioso** o **software malintencionado** es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático es utilizado en muchas ocasiones de forma incorrecta para referirse a todos los tipos de malware, incluyendo los verdaderos virus.

El software es considerado malware basándose en los efectos que cause en un computador, pensados por autor a la hora de crearlo. El término malware incluye virus, gusanos, troyanos, la mayoría de los rootkits, spyware, adware intrusivo, crimeware y otros software maliciosos e indeseables.

Según Panda Security, en los primeros meses de 2011 se han creado 73.000 nuevos ejemplares de amenazas informáticas por día, 10.000 más de la media registrada en todo el año 2010. De éstas, el 70% son troyanos, y crecen de forma exponencial los del sub tipo downloaders.

## Virus

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.

## Troyano

Es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños.

Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos crean una puerta trasera (en inglés *backdoor*) que permite la administración remota a un usuario no autorizado.

Un troyano no es estrictamente un virus informático, y la principal diferencia es que los troyanos no propagan la infección a otros sistemas por sí mismos.

Los troyanos están diseñados para permitir a un individuo el acceso remoto a un sistema. Una vez ejecutado el troyano, el individuo puede acceder al sistema de forma remota y realizar diferentes acciones sin necesitar permiso. Las acciones que el individuo puede realizar en el equipo remoto dependen de los privilegios que tenga el usuario en el ordenador remoto y de las características del troyano.

Algunas de las operaciones que se pueden llevar a cabo en el ordenador remoto son:

1. Utilizar la máquina como parte de una botnet (por ejemplo para realizar ataques de denegación de servicio o envío de spam).
2. Instalación de otros programas (incluyendo otros programas maliciosos).
3. Robo de información personal: información bancaria, contraseñas, códigos de seguridad.
4. Borrado, modificación o transferencia de archivos (descarga o subida).
5. Ejecutar o terminar procesos.
6. Apagar o reiniciar el equipo.
7. Monitorizar las pulsaciones del teclado.
8. Realizar capturas de pantalla.
9. Ocupar el espacio libre del disco duro con archivos inútiles.
10. Borra el disco duro

## Características de los troyanos

Los troyanos están compuestos principalmente por tres programas: un cliente, que envía las órdenes que se deben ejecutar en la computadora infectada, un servidor situado en la computadora infectada, que recibe las órdenes del cliente, las ejecuta y casi siempre devuelve un resultado al programa cliente y, por último, un editor del servidor, el cual sirve para modificarlo, protegerlo mediante contraseñas, unirlo a otros programas para que, al abrir el programa también se ejecute el servidor, configurar en que puerto deseamos instalar el servidor, etc. Atendiendo a la forma en la que se realiza la conexión entre el cliente y el servidor se pueden clasificar en:

Conexión directa (el cliente se conecta al servidor).

Conexión inversa (el servidor se conecta al cliente).

## Formas de infectarse con troyanos

La mayoría de infecciones con troyanos ocurren cuando se ejecuta un programa infectado con un troyano. Estos programas pueden ser de cualquier tipo, desde instaladores hasta presentaciones de fotos. Al ejecutar el programa, este se muestra y realiza las tareas de forma normal, pero en un segundo plano y al mismo tiempo se instala el troyano. El proceso de infección no es visible para el usuario ya que no se muestran ventanas ni alertas de ningún tipo.

**Gusanos**

Un **gusano** (también llamados IWorm por su apocope en inglés, *I* de Internet, *Worm*de gusano) es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

Los gusanos se basan en una red de computadoras para enviar copias de sí mismos a otros nodos (es decir, a otras terminales en la red) y son capaces de llevar esto a cabo sin intervención del usuario propagándose, utilizando Internet, basándose en diversos métodos,
como SMTP, IRC, P2P entre otros.

## Spyware

Es un programa que funciona dentro de la categoría malware, que se instala furtivamente en un ordenador para recopilar información sobre las actividades realizadas en éste. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante. Dado que el spyware usa normalmente la conexión de una computadora a Internet para transmitir información, consume ancho de banda, con lo cual, puede verse afectada la velocidad de transferencia de datos entre dicha computadora y otra(s) conectada(s) a la red

Entre la información usualmente recabada por este software se encuentran: los mensajes, contactos y la clave del correo electrónico; datos sobre la conexión a Internet, como la dirección IP, el DNS, el teléfono y el país; direcciones web visitadas, tiempo durante el cual el usuario se mantiene en dichas web y número de veces que el usuario visita cada web; software que se encuentra instalado; descargas realizadas; y cualquier tipo de información intercambiada, como por ejemplo en formularios, con sitios web, incluyendo números de tarjeta de crédito y cuentas de banco, contraseñas, etc.

Los cookies son archivos en los que almacena información sobre un usuario de internet en su propio ordenador, y se suelen emplear para asignar a los visitantes de un sitio de Internet un número de identificación individual para su reconocimiento subsiguiente. La existencia de los cookies y su uso generalmente no están ocultos al usuario, quien puede desactivar el acceso a la información de los cookies; sin embargo, dado que un sitio Web puede emplear un identificador cookie para construir un perfil de un usuario y que dicho usuario no conoce la información que se añade a este perfil, se puede considerar al software que transmite información de las cookies, sin

que el usuario consienta la respectiva transferencia, una forma de spyware. Por ejemplo, una página con motor de búsqueda puede asignar un número de identificación individual al usuario la primera vez que visita la página, y puede almacenar todos sus términos de búsqueda en una base de datos con su número de identificación como clave en todas sus próximas visitas (hasta que el cookie expira o se borra). Estos datos pueden ser empleados para seleccionar los anuncios publicitarios que se mostrarán al usuario, o pueden ser transmitidos (legal o ilegalmente) a otros sitios u organizaciones.

## Adware

Un programa de clase **adware** es cualquier programa que automáticamente se ejecuta, muestra o baja publicidad web al computador después de instalar el programa o mientras se está utilizando la aplicación. 'Ad' en la palabra 'adware' se refiere a 'advertisement' (anuncios) en inglés.

Algunos programas adware son también shareware, y en estos los usuarios tiene la opción de pagar por una versión registrada o con licencia, que normalmente elimina los anuncios.

Se han criticado algunos programas adware porque ocasionalmente incluyen código que realiza un seguimiento de información personal del usuario y la pasa a terceras entidades, sin la autorización o el conocimiento del usuario. Esta práctica se conoce como spyware, y ha provocado críticas de los expertos de seguridad y los defensores de la privacidad, incluyendo el Electronic Privacy Information Center. Otros programas adware no realizan este seguimiento de información personal del usuario.

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

Los anuncios emergentes aparecen durante la navegación web en el navegador como una ventana emergente o también durante el uso de programa del ordenador. Esta publicidad es molesta en algunos casos, pero lo que más molesta es que deteriora el rendimiento del sistema. El adware también puede recopilar información del usuario, lo que provoca preocupación por la privacidad.

## Pishing

***Phishing*** es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).
El estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Dado el creciente número de denuncias de incidentes relacionados con el *phishing*, se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica y campañas para prevenir a los usuarios con la aplicación de medidas técnicas a los programas.

### HTTPS

Hyper Text Transfer Protocol Secure (en español: *Protocolo seguro de transferencia de hipertexto*), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hiper Texto, es decir, es la versión segura de HTTP.

Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

El sistema HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. De este modo se consigue que la información sensible (usuario y claves de paso normalmente) no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

El puerto estándar para este protocolo es el 443.

### VPN

Una **red privada virtual**, **RPV**, o **VPN** de las siglas en inglés de ***Virtual Private Network***, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

## Características básicas de la seguridad

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación, integridad de toda la comunicación:

- Autentificación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- Integridad: de que los datos enviados no han sido alterados. Para ello se utiliza *funciones de Hash*. Los algoritmos de hash más comunes son los *Message Digest* (MD2 y MD5) y el *Secure Hash Algorithm* (SHA).

- Confidencialidad: Dado que sólo puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como *Data Encryption Standard*(DES), Triple DES (3DES) y *Advanced Encryption Standard* (AES).

- No repudio: es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él o ella.

## HTML5

**HTML5** (***H**yper**T**ext **M**arkup**L**anguage*, versión 5) es la quinta revisión importante del lenguaje básico de la World Wide Web, HTML. HTML5 especifica dos variantes de sintaxis para HTML: un «clásico» HTML (text/html), la variante conocida como *HTML5* y una variante XHTML conocida como sintaxis *XHTML5* que deberá ser servida como XML (XHTML) (application/xhtml+xml). Esta es la primera vez que HTML y XHTML se han desarrollado en paralelo.

Todavía se encuentra en modo experimental, lo cual indica la misma W3C; aunque ya es usado por múltiples desarrolladores web por sus avances, mejoras y ventajas.

Al no ser reconocido en viejas versiones de navegadores por sus nuevas etiquetas, se le recomienda al usuario común actualizar a la versión más actual, para poder disfrutar de todo el potencial que trae HTML5.

El desarrollo de este código es regulado por el Consorcio W3C.

## W3C

El **World Wide Web Consortium**, abreviado **W3C**, es un consorcio internacional que produce recomendaciones para la World Wide Web. Está dirigida por Tim Berners-Lee, el creador original de URL (*Uniform Resource Locator*, Localizador Uniforme de Recursos), HTTP (*HyperText Transfer Protocol*, Protocolo de Transferencia de HiperTexto) y HTML (Lenguaje de Marcado de HiperTexto) que son las principales tecnologías sobre las que se basa la Web.

La organización fue creada el 1 de octubre de 1994 por Tim Berners-Lee en el MIT, actual sede central del consorcio. Uniéndose posteriormente en abril de 1995 INRIA en Francia, reemplazado por el ERCIM en el 2003 como el huésped europeo del consorcio y Universidad de Keiō (Shonan Fujisawa Campus) en Japón en septiembre de 1996 como huésped asiático. Estos organismos administran el consorcio, el cual está integrado por:

Miembros del W3C. A abril de 2010 contaba con 330 miembros.

Equipo W3C (W3C Team) 65 investigadores y expertos de todo el mundo.

Oficinas W3C (W3C Offices). Centros regionales establecidos en Alemania y Austria (oficina conjunta), Australia, Benelux (oficina conjunta), China, Corea del Sur, España, Finlandia, Grecia,

Hong Kong, Hungría, India, Israel, Italia, Marruecos, Suecia y Reino Unido e Irlanda (oficina conjunta).

## Web 2.o

El término **Web 2.0** está asociado a aplicaciones web que facilitan el compartir información, la interoperabilidad, el diseño centrado en el usuario y la colaboración en la World Wide Web. Ejemplos de la Web 2.0 son las comunidades web, los servicios web, las aplicaciones Web, los servicios de red social, los servicios de alojamiento de videos, las wikis y blogs.

Aunque el término sugiere una nueva versión de la World Wide Web, no se refiere a una actualización de las especificaciones técnicas de la web, sino más bien a cambios acumulativos en la forma en la que desarrolladores de software y usuarios finales utilizan la Web. El hecho de que la Web 2.0 es cualitativamente diferente de las tecnologías web anteriores ha sido cuestionado por el creador de la World Wide Web Tim Berners-Lee, quien calificó al término como "tan sólo una jerga"- precisamente porque tenía la intención de que la Web incorporase estos valores en el primer lugar.

Antes de la llegada de las tecnologías de la Web 2.0 se utilizaban páginas estáticas programadas en HTML (Hyper Text Markup Language) que no eran actualizadas frecuentemente. El éxito de las .com dependía de webs más dinámicas (a veces llamadas *Web 1.5*) donde los sistemas de gestión de contenidos servían páginas HTML dinámicas creadas al vuelo desde una base de datos actualizada. En ambos sentidos, el conseguir *hits* (visitas) y la estética visual eran considerados como factores importantes.

Los teóricos de la aproximación a la Web 2.0 piensan que el uso de la web está orientado a la interacción y redes sociales, que pueden servir contenido que explota los efectos de las redes, creando o no webs interactivas y visuales. Es decir, los sitios Web 2.0 actúan más como puntos de encuentro o webs dependientes de usuarios, que como webs tradicionales.

En general, cuando mencionamos el término Web 2.0 nos referimos a una serie de aplicaciones y páginas de Internet que utilizan la inteligencia colectiva para proporcionar servicios interactivos en red.

Para compartir en la Web 2.0 se utilizan una serie de herramientas, entre las que se pueden destacar:

Blogs: La blogosfera es el conjunto de blogs que hay en internet. Un blog es un espacio web personal en el que su autor (puede haber varios autores autorizados) puede escribir cronológicamente artículos, noticias (con imágenes y enlaces), pero además es un espacio colaborativo donde los lectores también pueden escribir sus comentarios a cada uno de los artículos (entradas/post) que ha realizado el autor.

Wikis: En hawaiano "wikiwiki " significa: rápido, informal. Una wiki es un espacio web corporativo, organizado mediante una estructura hipertextual de páginas (referenciadas en un menú lateral), donde varias personas elaboran contenidos de manera asíncrona. Basta pulsar el botón "editar" para acceder a los contenidos y modificarlos. Suelen mantener un archivo histórico de las versiones

anteriores y facilitan la realización de copias de seguridad de los contenidos. Hay diversos servidores de wiki gratuitos.

Entornos para compartir recursos: Todos estos entornos nos permiten almacenar recursos en Internet, compartirlos y visualizarlos cuando nos convenga desde Internet. Constituyen una inmensa fuente de recursos y lugares donde publicar materiales para su difusión mundial.

Documentos: podemos subir nuestros documentos y compartirlos, embebiéndolos en un Blog o Wiki, enviándolos por correo.

Videos: Al igual que los Documentos, anteriormente mencionados, se pueden "embeber" un video tomado de algún repositorio que lo permita, tal como YouTube.

Presentaciones

Fotos

Plataformas educativas

Aulas virtuales (síncronas)

Redes Sociales.

## Web 3.0 o Web Semántica

Aún no existe total consenso acerca de lo que significa la Web 3.0, aunque se lo asocia al término Web Semántica, acuñado por Tim Berners-Lee, y hay coincidencia acerca de que en esta etapa del desarrollo de Internet se añadirá significado a la web, aunque no hay acuerdo sobre cuáles son los caminos más apropiados para su desarrollo.

**Ideas en torno a la definición de la Web 3.0**

Básicamente, tienen que ver con los avances y proyectos en curso que tienden a una cada vez mayor y más eficiente incorporación de la web a la cotidianidad. Se habla así, de conceptos tales como: Web 3D, Web centrada en multimedia y Web permanente.

**¿Qué es la Web Semántica?**

Nadie mejor que Tim Berners-Lee, el creador de la World Wide Web, para dar respuesta a este interrogante. La denominación de Web Semántica se remonta al año 2001, cuando presentó en Scientific American el ya famoso caso de Lucy.

Sin embargo, en una entrevista publicada por BusinessWeek, en abril de 2011, señala que quizás debería haberla llamado Web de los datos, dado que la palabra semántica es utilizada para significar diferentes cosas.

¿En qué consiste la Web de los datos y para qué puede ser utilizada?

Básicamente, la idea se refiere a una web capaz de interpretar e interconectar un número mayor de datos, lo que permitiría un avance importante en el campo del conocimiento.

En tal sentido, Berners-Lee destaca lo que esta transformación traería aparejada en el campo de la investigación genética y el tratamiento farmacológico de enfermedades hasta ahora incurables. Diseñada correctamente, la Web Semántica puede asistir a la evolución del conocimiento humano en su totalidad.

La Web Semántica es una Web de datos - de las fechas y los títulos y números de pieza y las propiedades químicas y cualquier otro dato que se podría concebir. La colección de tecnologías semánticas Web (RDF, OWL, SKOS, SPARQL, etc) proporciona un entorno donde la aplicación puede consultar los datos, extraer inferencias utilizando vocabularios, etc

Sin embargo, para hacer la Web de Datos de una realidad, es importante contar con la enorme cantidad de datos en la Web disponibles en un formato estándar, accesible y manejable por las herramientas de la Web Semántica. Además, no sólo de la Web Semántica necesitan tener acceso a los datos, pero *las relaciones entre los datos* deben estar disponibles también para crear una *Web* de datos (en lugar de una colección enorme de conjuntos de datos). Esta colección de conjuntos de datos interrelacionados en la Web también puede ser referido como Linked Data.

Para lograr y crear Linked Data, las tecnologías deben estar disponibles para un formato común (RDF), ya sea para hacer la conversión o en la marcha el acceso a bases de datos existentes (relacionales, XML, HTML, etc.)También es importante ser capaz de configurar consultas, criterios de valoración para acceder a los datos con mayor comodidad. W3C ofrece una gama de tecnologías (RDF, GRDDL, polvo, RDFa, la próxima R2RML, RIF, SPARQL) para obtener acceso a los datos.

Fuentes: World Wide Web Consortium, Hello Google, Google webmasters, Wikipedia, Maestros de la Web