

## **1.- ¿Qué es el Correo Electrónico?**

En su forma más sencilla, el CORREO ELECTRÓNICO, también llamado E-MAIL (Electronic Mail), es una forma de enviar correo, mensajes o cartas electrónicas de un ordenador a otro. Tanto la persona que envía el correo electrónico, como la persona que lo recibe, debe tener una cuenta de correo en INTERNET.

El E-MAIL fue uno de los primeros servicios que ofreció la red ARPANET. Esto no quiere decir que sea un servicio exclusivo de la red INTERNET. El E-MAIL es un servicio que ofrece prácticamente todo tipo de redes existentes. La diferencia es la forma de ese E-MAIL, que en muchos casos será diferente para las distintas redes.

El E-MAIL es mucho más rápido que el correo tradicional. Cuando se envía correo electrónico, puede ser cuestión de minutos que llegue a su destino, sea cual sea el lugar del mundo donde se encuentre el destinatario del mensaje. El mensaje electrónico pasa de un servidor a otro. Cada servidor que recibe un mensaje, comprueba la dirección y lo envía por la ruta correcta a otro servidor. Este proceso se repite hasta que el mensaje llega al servidor de destino, entonces se almacena en el buzón electrónico correspondiente (espacio de disco destinado a almacenar el correo electrónico de un usuario de dicho servidor). Sin embargo con el correo tradicional suele ser cuestión de días, semanas e incluso meses.

Las características del E-MAIL que añaden mas funcionalidad son:

Es posible organizar el correo en CARPETAS. Si el volumen de correo recibido es grande, será necesario almacenar ese correo por temas, por usuarios, etc. Seria algo parecido a almacenar ficheros en directorios.

Es posible la RETRANSMISIÓN DE MENSAJES que nos llegan hacia otras direcciones de correo.

Lo normal en los sistemas actuales de correo, es la posibilidad de dar REPLICA a un mensaje que nos ha llegado. Consiste en responder a un mensaje basándonos en el que nos ha llegado, tomando datos de este.

Hay muchas mas características que dan mayor funcionalidad a un sistema de correo electrónico, pero estas son las más habituales. Además dichas posibilidades dependen del software de correo electrónico usado en cada caso.

### **Tipos de Correo Electrónico**

#### *Correo POP*

Este tipo de correo se hace a través de una conexión a internet, pero sin necesidad de estar conectado permanentemente a la red, simplemente se conecta a través de un módem o ASDL a un servidor dedicado de correo (llamado POPSERVER), y éste se conecta para recibir, enviar los mensajes que estén en nuestro buzón o casilla de correo y corta la comunicación. Esto se hace a través de programas específicos (Outlook Express, Eudora, Pegasus Mail, Nescape Communicator, etc.) Los mensajes se borran del servidor y se almacenan en el disco rígido de la PC del usuario. Tenemos capacidad ilimitada de almacenar mails, es más rápido y los mensajes se pueden escribir y leer sin necesidad de estar conectados a la red, los podemos consultar en cualquier momento, redactarlos y enviarlos mas tarde. Sólo nos conectamos para enviar y recibir. Las DESVENTAJAS son: generalmente no podemos consultar nuestro los mensajes recibidos desde otras PC o vía Web, hay mayor posibilidad de ingreso de virus, es mas difícil combatir y filtrar el SPAM. Las VENTAJAS: es mas rápido, mas accesible a los mensajes, se lee y escribe sin conexión

#### *Web Mail o Correo Web*

Este es un servicio de correo generalmente gratuito que se encuentra en portales y/o buscadores (HOTMAIL, YAHOO, GMAIL, UOL, UBB, etc.) que ofrecen este servicio, en donde un usuario se suscribe (define su nombre de usuario o ID y contraseña), y obtiene su casilla de correo personal.

Para usar este tipo de correo es imprescindible contar con UNA CONEXIÓN a Internet (paga o gratis) y un navegador o browser. Para leer y escribir hay que estar permanentemente conectado (ONLINE), es lento, y la cantidad de mails que almacena están limitados, el tamaño de los archivos que se envían, etc. Los mensajes quedan en el servidor donde está alojada la cuenta de correo Web (en el disco rígido del servidor de correo).

Para utilizar este correo sólo hace falta el navegador o browser, ya que, al entrar al servicio, se convierte en el administrador de correo. Las VENTAJAS: tienen filtros antispam y antivirus, se puede consultar desde cualquier PC (locutorio, ciber, etc.) DESVENTAJAS: hay que estar permanentemente conectado, es mas lento, tiene propagandas, es mas inseguro.

### **¿Qué es un USUARIO ?**

Un usuario es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado un password u contraseña para poder acceder a su cuenta.

### **¿Qué es un PROVEEDOR o ISP?**

El proveedor o ISP (Internet Service Provider) es aquel que instala y se conecta en forma directa y permanente con equipos especiales a la red, instala un servidor de navegación y un servidor de correo (POPSERVER), y brinda el acceso a la red a través de sus líneas telefónicas, banda ancha, ASDL, cablemodem, fibra óptica. Generalmente está dentro del radio de la localidad del usuario para que el costo de la llamada sea local. Nos asigna un nombre

de usuario y un código de seguridad (password) para poder ingresar a la red.

**¿Cómo nos conectamos a la RED?**

Existen varias formas de conectarnos al proveedor

- Conexiones permanentes o dedicadas
- Conexiones directas o terminal por conmutación telefónica (PPP)

*Conexiones permanentes o dedicadas*

Significa que se trata de una conexión directa a una computadora ( con una gran capacidad de procesar y almacenar datos ) conectada directamente a una red TCP/IP que forman la red Internet. Esto lo logramos a través del sistema ASDL, Fibra Optica, Speedy, Fibertel o cablemodem. Donde TCP significa Protocolo de Control de Transmisión y IP Protocolo Internet.

Aquí la computadora está permanentemente conectada a la red, sin costos adicionales de llamadas telefónicas. se paga un abono mensual por el servicio, y requiere de una placa específica.

*Conexiones por conmutación telefónica*

Este tipo de conexión se conoce con el nombre PPP. Donde PPP significa Protocolo Punto a Punto. Se debe utilizar la línea telefónica a través de un módem y comunicarse con un proveedor del servicio Internet o ISP (Arner, Ciudad Digital, UoISinectis, Netizen, etc.), convirtiendo su PC en una terminal de la computadora del proveedor llamada Anfitriona o Server (servidor).

Se paga como una llamada común o si se dispone de una cuenta especial se obtienen tarifas preferenciales

**2.- Estructura de un mensaje de Correo Electrónico**

En lo que se refiere a la estructura de un mensaje de correo electrónico o E-MAIL, es muy parecida a la estructura de una carta normal del correo tradicional. Diferenciamos dos partes fundamentales, la cabecera y el cuerpo del mensaje:

La CABECERA actúa como de matasellos electrónico, de tal forma que cuando un usuario recibe un mensaje, puede saber a través de la información de la cabecera, quien le envió el mensaje, como fue enviado y cuando.

- Nombre o dirección del usuario que envía el mensaje (FROM o DE) cuando se tiene mas de una cuenta.
- Nombre o dirección del usuario que recibirá el mensaje (TO o PARA o A)
- Nombre o dirección de las copias del mensaje (CC o Con Copia)
- Nombre o dirección de las copias del mensaje ocultas (CCO o Con Copia Oculta)
- Tema o asunto del mensaje (SUBJECT o ASUNTO). Otro ejemplo de cabecera

<b>A:</b>	<input type="text"/>
<b>Cc:</b>	<input type="text"/>
<b>Cco:</b>	<input type="text"/>
<b>Asunto:</b>	<input type="text"/>

El CUERPO (BODY) del mensaje es la parte correspondiente al contenido del mensaje, que puede ser texto, imágenes, texto con formato y en ocasiones ficheros asociados.

**3.- Direcciones de Correo Electrónico**

Una dirección de correo electrónico es la forma que tenemos de especificar al programa de correo electrónico, el lugar o persona a la que queremos enviar el mensaje en concreto. La dirección de correo electrónico tiene la siguiente forma:

**andres@uolsinectis.com.ar**

**usuario@dominio.organización.país**

**1      2      3                      4                      5**

- 1.- USUARIO:  
También se lo llama nombre de usuario o ID en caso de ser una cuenta de e-mail la elegimos nosotros
- 2.- ARROBA:  
Es el símbolo que separa el nombre de usuario del nodo o dominio. Este símbolo identifica el correo por Internet
- 3.- DOMINIO:  
El nombre del proveedor o dominio identifica la ruta o máquinas designadas para el envío y recepción de mensajes de forma correcta a través de Internet

**4.- ORGANIZACION:**

Identifica a que tipo de organización (educación, comercial, militar, etc).

**5.- EXTENSION DE PAIS:**

Identifica el país donde se haya alojado el dominio. Si el servidor no está en EEUU se le asignan dos letras para identificar los países.

Primero se pone el nombre del usuario, indica el buzón de correo electrónico correspondiente a la persona a la que va destinado el mensaje. Después se pone un símbolo que se denomina arroba. A continuación se pone el nombre de la máquina o nombre del servidor donde tiene cuenta el usuario y por ultimo se pone un punto seguido del tipo de dominio al que pertenece la máquina (.com, .org, .net, etc.)

Hay varios tipos de dominios en Internet. Normalmente suelen tener como máximo 3 letras que los identifican. A continuación explico algunos:

.com: para un negocio o una empresa internacional

.edu: para una Universidad o centro de educación

.org: para una organización no comercial

.gov: para una agencia u oficina gubernamental

.mil: para una institución militar

.net: para una red determinada

En otras ocasiones se pone un indicativo del país donde esta situado el servidor geográficamente hablando:

.es: España

.uk: Reino Unido

.it: Italia

.ar: Argentina

Hay nuevos tipos de organizaciones como: .tv, .htm, .info, etc

**4.- Archivos asociados a los mensajes electrónicos**

Podemos adjuntar cualquier tipo de archivo al cuerpo del mensaje de correo. Imágenes (JPG,GIF,TIFF,etc), texto (DOC,TXT, etc) música (MP3).

Muchas veces se utiliza un software para comprimir el archivo a adjuntar, de esta manera se reduce el tamaño en Kb que ocupa, y se hace mas rápida la transferencia y ocupa menos espacio en nuestra casilla o buzón.

El software mas utilizado para esto se llama WINZIP y genera archivos con la extensión .ZIP. Para poder comprimir y descomprimir archivos es necesario tener instalado el software. No solo se usa para envío de correo, también para comprimir y liberar espacio en el disco rígido.

Otro tipo de archivos asociados a mails, y que especialmente se encuentran en páginas Webs, son los PDF o formato de documentos portátiles (PDF, Portable Document Format). Este tipo de archivo está comprimido y encriptado, puede poseer imágenes, tiene formato, se puede imprimir, etc. Se utiliza mucho para leer y presentar en internet información, trabajos, tesis, monografías, documentos, etc. Para poder visualizar y trabajar con archivos en formato PDF es necesario tener instalado en la PC un programa llamado *ACROBAT READER*. Es un programa *FREE* que se puede descargar de Internet desde varios sitios, también viene incluido en mucho Cds de uso comercial o promocionales

**5.- Listas de correo**

Las LISTAS DE CORREO son grupos de usuarios en los que se producen discusiones o debates públicos o privados, en los que puede participar cualquier que disponga de una cuenta de correo. Cada LISTA DE CORREO contiene una lista de los usuarios a los que les interesa un mismo tema, idea o tópico.

El funcionamiento es de la siguiente forma: cuando uno de los miembros de una lista de correo envía una carta a la lista de correo, esta carta se distribuye a todos los demás miembros de la lista de correo. De esta forma, todos pueden conocer como se avanza en el debate sobre el tema en cuestión. Cuando el usuario envía la respuesta, esta se distribuye igualmente a todos los demás. Un miembro de una lista de correo, puede participar abiertamente en ella enviando nuevos mensajes, respondiendo a otros mensajes o bien puede solo leer los mensajes sin participar en el debate.

Para la distribución de todos los mensajes que se producen en una lista de correo (que puede llegar a ser muy grande y abarcar a usuarios distribuidos por todo el mundo), se necesitan unos programas especializados denominados MLM (Administradores de listas de correo). Los dos programas más usados frecuentemente son: Listserv, Majordomo y mailman.

Las LISTAS DE CORREO tienen varias ventajas sobre los GRUPOS DE NOTICIAS o NEWS. Una de ellas es que no es necesario ir a buscar el grupo en donde se encuentra el tema, el contenido del debate se envía automáticamente a la dirección de correo electrónico. Otra de las ventajas es que cada usuario se suscribe a la lista de correo con el tema de discusión que a uno le interesa. Una ventaja mas es que para participar en las listas de correo solo se necesita una cuenta de correo electrónico, mientras que para usar las NEWS se necesitan programas adicionales.

Para subscribirse a una lista de correo lo único que hay que hacer es enviar un mensaje electrónico al administrador de la lista en cuestión. Este administrador añadirá al usuario a la lista de correo y responderá enviando la información necesaria para participar en el debate. Para darse de baja en una lista de correo lo único que hay que hacer es enviar un nuevo mensaje al administrador pidiendo la baja de la lista.

## **6.- Protocolos que intervienen en una aplicación de Correo Electrónico**

### **¿Qué es el protocolo SMTP**

SMTP (Simple Mail Transfer Protocol). Es el protocolo para la entrega de mensajes entre sistemas (servidores) de Internet.

El significado de las siglas de SMTP es Protocolo Simple de Transmisión de Correo (Simple Mail Transfer Protocol). Este protocolo es el estándar de Internet para el intercambio de correo electrónico entre servidores, y envío entre usuario y servidor.

### **¿Qué es el protocolo POP**

El significado de las siglas POP es Protocolo de Oficina de Correos (Post Office Protocol).

Este modelo de comunicaciones se basa en el concepto de buzón. Al igual que ocurre en una oficina de correos local, de una ciudad, tiene un espacio para almacenar el correo hasta que se recojan. De igual manera el servidor POP almacena el correo electrónico en buzones hasta que un programa cliente lo recupera.

El cliente POP se conecta con el servidor. Una vez que se ha entrado en el sistema, el cliente POP puede dialogar con el servidor para conocer si tiene correo, cuantos mensajes tiene, que se los envíe (bajar el correo o descargar los mensajes), que los borre, etc.

La situación actual es que se utiliza el protocolo SMTP para el envío de correo y para la recepción de correo se utiliza el protocolo POP, pero ya en su tercera versión desde su aparición, el POP3.

## **Netiquette**

Lo cortés no quita lo valiente", dice un viejo refrán que perfectamente podría *aggiornarse* a la comunicación en Internet y, de esa manera, refrescar normas básicas de comportamiento on line, que parecen haberse olvidado en el mundo virtual.

.Pese a que millones de personas se conectan diariamente por medio del correo electrónico, chats, foros, servicios de mensajes instantáneos y, los más recientes, weblogs, son muy pocos los que cumplen con la denominada "netiquette" -o etiqueta en la Red (Net)- que indica el comportamiento que debe expresarse en el ciberespacio para lograr una comunicación efectiva con el resto de los usuarios.

.La "netiquette" está compuesta por una serie de reglas que surgieron hace aproximadamente 20 años, cuando la red de redes no estaba muy difundida. Estas normas fueron cambiando y adaptándose a las nuevas necesidades y servicios de la web y, aunque no son obligatorias, la práctica de estos "buenos modales" ayudan a que la convivencia en el espacio virtual sea más armónica.

.Si bien hay reglas específicas para cada servicio en particular, hay algunas más generales que se aplican a cualquier actividad online. En la web pueden encontrarse varios sites que explican cuáles son las conductas que debemos adoptar frente al monitor.

.No está de más tener en cuenta algunas de estas normas básicas, propuestas por manuales especializados de las páginas [www.links.org.ar/infoteca/Netiquet.rtf](http://www.links.org.ar/infoteca/Netiquet.rtf) y <http://www.albion.com/> , que son:

- . Recordar siempre que hay seres humanos del otro lado de la PC y que no se está hablando con una máquina
- . Ser práctico y conciso en los mensajes
- . Ser cortés: si se participa en un chat o en un foro de discusión, hay que saludar al resto del grupo
- . Evitar los insultos y ataques
- . No enviar mensajes cuando se está enojado
- . Evitar enviar archivos adjuntos demasiado pesados, en especial cuando no fueron solicitados por el destinatario.
- . Contestar los e-mails entre las 24 y 48 horas de recibido el mensaje
- . En los foros, abstenerse de escribir mensajes que no correspondan al tema propuesto
- . Utilizar el reply del correo electrónico cuando contestamos (en lugar de escribir uno nuevo) pero borrar el original para que no se repita (de esa manera no se sobrecarga la Red)
- . Los mensajes en MAYÚSCULA equivalen a gritarle al destinatario
- . No corregir los errores de ortografía ajenos
- . Nunca enviar una carta en cadena por e-mail: este tipo de mensajes son muy molestos y en la mayoría de los casos son falsos
- . Cuando se responde un mensaje que originalmente tenía varios destinatarios además de uno mismo, borrar las direcciones de correo de las personas a la que no incumba la respuesta

- . Siempre utilizar el "subject" para aclarar el asunto del correo electrónico
- . Respetar el copyright del material que se reproduce, como así también las referencias a los autores
- . Ser discreto con la información personal o privada, ya sea propia o de terceros
- . Respetar las culturas diferentes a la nuestra
- . Tener en cuenta estas pautas al conectarse a Internet sirve para lograr una comunicación online más respetuosa y amena y, de paso, ayuda a evitar los malentendidos, propios de las relaciones que no se dan cara a cara.

## **SPAM**

### **1. ¿Qué es el SPAM?**

SPAM es correo electrónico no solicitado o no deseado que se envía a múltiples usuarios con el propósito de hacer promociones comerciales, publicidad, o proponer ideas. SPAM también es conocido como e-mail comercial no solicitado.

Generalmente, los mensajes spam son publicidad, ofertas por asistencia financiera o para tentar al usuario a visitar cierta página web. Estos mensajes son enviados a cientos de miles de usuarios cada vez. Esto ocurre vía una lista legítima de mailing.

### **2. ¿Por qué no es correcto hacer SPAM?**

El spam es un robo de recursos. Enviar e-mails no le cuesta casi nada a la persona que los envía; el usuario toma todos los costos. Cuando un usuario recibe una docena de mensajes spam en una semana, el costo no es tan obvio, sin embargo, cuando uno multiplica ese tráfico de mensajes por cientos de miles en un entorno corporativo, se torna realmente molesto. El spam no sirve como interés corporativo. Utiliza el CPU, toma espacio en el disco del servidor y en el disco de los usuarios finales. La distribución del spam puede causar pérdida de ancho de banda en la red. Además, la distribución del spam puede multiplicar el riesgo de distribución de ataques de virus simultáneamente exponiendo el mismo archivo infectado a miles de usuarios. Existen muchos ejemplos de virus Troyanos que son enviados como archivos adjuntos en lista de mailing. Cuanto más grande sea la lista de mailing spam, más son los problemas asociados con la seguridad.

### **3. ¿Cómo llegó mi nombre a una lista de mailing SPAM?**

Los que envían spam construyen sus listas utilizando varias fuentes. Algunos utilizan programas que recogen direcciones de e-mail. Otros recogen direcciones de otras listas de suscriptores. Otros también utilizan buscadores web que buscan dentro del código HTML los tags "mailto:". También pueden ser recogidos desde directorios de e-mail on-line. Inclusive desde una sesión de chat. La lista de mailing spam también pudo haber sido comprada a un vendedor legítimo al cual usted le dio su dirección de e-mail al comprar algún servicio o al registrarse en una encuesta. También son extraídas de las cadenas de mensajes que se envían sin escribir las direcciones con CCO (Con Copia Oculta) o borrar los otras direcciones de CC (Con Copia)

## **HOAX**

Un hoax se puede definir como una falsa alarma sobre un virus informático o mensajes de correo sobre ayuda, enfermedades, niños en con enfermedades terminales, mensajes de suerte, etc. que se distribuye en cadena de mensajes por correo electrónico. Estas cadenas involucran cada vez más y más usuarios ya que el mensaje sugiere al receptor reenviar la información a todas las direcciones de correo posibles. Algunos ejemplos de virus hoax de este tipo son el "Pen Pal Greetings", el "Good Times", Las Ranas de budwaiser, Jessica, Niño con cancer, etc., que intentan generar pánico o solidaridad entre los usuarios de Internet utilizando argumentos falsos y generalmente relacionados con virus informáticos o desgracias ajenas.

Sin duda, este tipo de "cadenas" son consideradas dañinas ya que muchas veces implican pérdida de productividad y tiempo de las personas que reciben estos mensajes. Algunos de los virus hoax más populares llevan más de tres años distribuyéndose de usuario en usuario, aunque importantes organizaciones dedicadas a la seguridad informática inviertan muchos recursos en desmentirlos. Aconsejamos a todos los usuarios que reciban este tipo de mensajes que se informen antes de alertar a otras personas.

Además de ser falsos, sirven para que los "piratas informáticos" recolecten direcciones de correo válidas, ya que cada uno le envía un correo a direcciones conocidas y que funcionan, luego estos las venden para producir SPAM.

## **¿Qué es un Virus?**

Un virus es un programa – una porción de código ejecutable – que tiene la habilidad única de reproducirse. Como los virus biológicos, los virus informáticos pueden diseminarse rápidamente y algunas veces son difíciles de erradicar. Se pueden adherir a cualquier tipo de archivo y se diseminan con los archivos que se copian y envían de persona a persona.

Además de reproducirse, algunos virus informáticos tienen algo en común: una rutina dañina, que el virus descarga como una bomba. Mientras que las descargas pueden ser simples mensajes o imágenes, éstas también pueden

borrar archivos, reformatear el disco duro o causar otro tipo de daño. Si el virus no contiene una rutina dañina, aún puede causar problemas, como tomar espacio libre del disco y de la memoria, y también disminuir el rendimiento de la computadora.

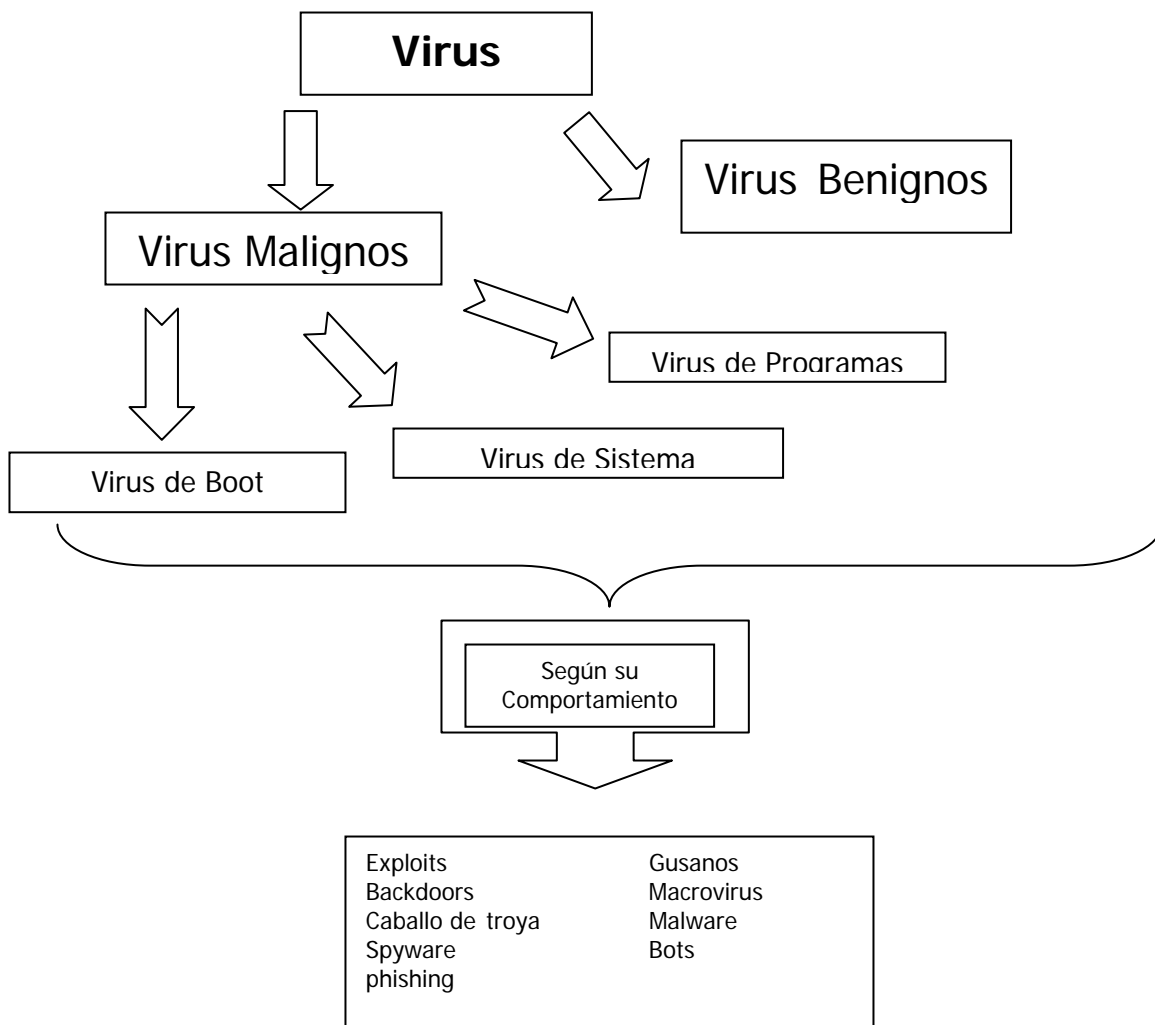
Hace varios años la mayoría de los virus se diseminaban vía disquette, pero el auge de Internet introdujo un nuevo mecanismo de distribución de virus. Con el e-mail, utilizado como la herramienta más importante de comunicación, los virus se están diseminando rápidamente. Los virus en los e-mails pueden infectar toda una empresa en cuestión de minutos, con un costo de millones de dólares anualmente en productividad perdida.

Existen una diversidad de virus, que afectan la información de miles de usuarios, atacan a las unidades de almacenamiento (discos rígidos, disquetes), a las computadoras, a la información organizada, etc. Se pueden clasificar de la siguiente manera:

Por la intención con que se manifiestan  
Definida en 1987, se clasifica a los virus en dos grupos:

a) *Virus Informáticos Benignos*. Por que no causan daños dramáticos y son fácilmente controlables. Consiste en un corto programa residente en memoria , sin consecuencia, que protagoniza una broma informática, nos informa de algún sonido alarmante, nos indica por pantalla algún mensaje desastroso , etc., pero todo no queda mas en un susto. El origen de estos virus es incierto, aunque los aquí denominados "benignos" parecen tener su origen en algunos clubs de software libre de Estados Unidos, en los cuales cualquier programador no profesional deposita sus programas y recibe donaciones voluntarias de los usuarios.

b) *Virus Informáticos Malignos*. Son los responsables de generar catastróficos desastres en los archivos con sistemas. Daña la pista de arranque (incluidos el sector). Deteriora ficheros, etc. A esta clasificación pertenecen la gran mayoría de virus que existen en la actualidad.



**Tipos de VIRUS según los sectores que ataca o afecta:**

*Virus de Boot*: Infectan la memoria y atacan el sector de arranque de los disquettes y el disco duro y desde cuya posición pueden lanzar arteros ataques a los archivos y áreas del sistema que su creador haya decidido afectar. Como el trágicamente famoso virus Michelangelo. Infectando y destruyen los programas de arranque de la PC.

*Virus de Sistema*: Producidos para infectar en primer lugar al command.com y posteriormente a otras áreas importantes del sistema como la primera o segunda FAT ( File Allocation Table = Tabla de Asignación de Archivos ) y la Tabla de Particiones (Master Boot Record). Los comandos del Sistema Operativo, como COPY, DIR o DEL, son programas que se introducen en la memoria al cargar el Sistema Operativo y es así como el virus adquiere el control para infectar todo disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver sus carpetas (también llamadas: folders, subdirectorios, directorios).

**Virus de Programas Ejecutables:** Atacan aquellos archivos de programas ejecutables, con extensión EXE y COM. A partir de 1988 los virus empezaron a infectar y averiar archivos de diferentes extensiones, tales como DBF, BIN, NTX, GIF, etc., con lo cual la clasificación anterior dejó de ser vigentes. Hoy en día los virus no infectan en forma específica y limitativa las áreas del sistema o a tipos de archivos. Lo hacen al libre albedrío de sus creadores, cuando quieren dejando de lado clasificaciones tradicionales. Los virus requieren ser ejecutados para lograr sus objetivos y por esa razón buscan adherirse únicamente a los archivos COM, EXE o SYS o a las áreas importantes del sistema, como el sector de arranque, memoria y tabla de particiones. Una vez activados atacaran a otros archivos ejecutables o áreas, haciendo copias de sí mismos, sobrescribiendo o alterando archivos de cualquier otra extensión, no ejecutables las extensiones diferentes a COM, EXE o SYS solamente servirán de anfitriones pasivos mas no activos, pudiendo quedar alterados o inutilizados pero jamás podrán contagiar a otros archivos.

### Tipos de VIRUS según su comportamiento:

**Caballo de Troya:** Son archivos o programas (el virus viene enmascarado como un archivo aparentemente inofensivo) que en su interior contienen códigos o subprogramas capaces de dañar la computadora que los porte. Similares a los virus, pero con la diferencia de que los troyanos no tienen la capacidad de autoinfectar la computadora, por lo que requieren que su "víctima" abra o ejecute un archivo anexo, generalmente, a un mensaje de correo electrónico para que de este modo el virus instale una copia de sí mismo y a partir de ello, empiece su proceso de infección..

**Gusanos (WORMS):** Programa codificado como accesorio en el correo electrónico, reproduciéndose a sí mismo, modificando o no al huésped y extendiéndose por vía de la red electrónica, sin necesidad de un programa que los transporte, a otros huéspedes. El fin de dicho programa es recopilar cierto tipo de información programada (tal como los archivos de passwords) para enviarla a un equipo determinado al cual el creador del virus tiene acceso o el de colapsar el sistema a causa de las numerosas replicaciones.

**Backdoors:** Son también conocidos como herramientas de administración remotas ocultas. Son programas que permiten controlar remotamente la PC infectada. Generalmente son distribuidos como troyanos y gusanos. Cuando un virus de estos es ejecutado, se instala dentro del sistema operativo, al cual monitorea sin ningún tipo de mensaje o consulta al usuario. Incluso no se lo ve en la lista de programas activos. Los Backdoors permiten al autor tomar total control de la PC infectada y de esta forma enviar, recibir archivos, borrar o modificarlos, mostrarle mensajes al usuario, etc.

**Macrovirus:** Usa la auto-ejecución de macros en una aplicación tipo office (Word, excel) para generar copias de sí mismo, tomar el control de las aplicaciones y ejecutar rutinas que producen distintos tipos de daños a la información y extenderse.

**Los bots** o "robots" son gusanos o troyanos automatizados cuya función es instalarse en los ordenadores para realizar de modo automático una determinada acción como el envío continuado de spam, convirtiendo a la máquina en lo que comúnmente se conoce como "zombi".

Muchos bots están diseñados para recibir y ejecutar las órdenes de un atacante remoto. De esta manera, en lugar de limitarse a realizar una sola acción, pueden llevar a cabo otras muchas dependiendo de los deseos de su autor (ataques a otras máquinas, descarga de otros códigos maliciosos en el ordenador, etc.). Por lo general, el objetivo de los creadores de bots no es instalarlos en una sola máquina, sino crear redes de bots, es decir, de máquinas infectadas con un determinado bot. Esto puede reportar grandes beneficios económicos ya que, por ejemplo, puede conseguirse que un ejemplar de spyware pueda ser instalado al mismo tiempo en un gran número de ordenadores para recoger millones de datos, que pueden ser vendidos a empresas a cambio de importantes cantidades de dinero.

Para instalar un bot en un sistema pueden emplearse medios como el aprovechamiento de vulnerabilidades en navegadores, que permitan la descarga y ejecución automática de archivos al visitar una página web. Así, su forma de distribución es el mayor peligro de los bots, ya que muchos ejemplares desconocidos se encuentran instalados en un gran número de máquinas en todo el mundo, sin que los usuarios ni las compañías de seguridad tengan constancia de su existencia. Dado que los antivirus tradicionales sólo pueden hacer frente a amenazas previamente conocidas, un bot desconocido escapa de su campo de acción.

**Exploit:** técnica o programa que aprovecha un fallo o hueco de seguridad -una vulnerabilidad- existente en un determinado protocolo de comunicaciones, sistema operativo, o herramienta informática.

**Spyware** Los programas espía, también conocidos como *spyware*, son aplicaciones informáticas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario. Los datos recogidos son transmitidos a los propios fabricantes o a terceros, bien directamente, bien después de ser almacenados en el ordenador.

El *spyware* puede ser instalado en el sistema a través de numerosas vías, entre las que se encuentran: troyano, que los instalan sin consentimiento del usuario; visitas a páginas web que contienen determinados controles ActiveX o código que explota una determinada vulnerabilidad; aplicaciones con licencia de tipo shareware o freeware descargadas de Internet, etc.

El *spyware* puede ser instalado con el consentimiento del usuario, pero en ocasiones no es así. Lo mismo ocurre con el conocimiento de la recogida de datos y la forma en que son posteriormente utilizados.

**Adware** es una palabra inglesa que nace de la contracción de las palabras *Advertising Software*, es decir, programas que muestran anuncios. Se denomina *adware* al *software* que muestra publicidad, empleando cualquier tipo de medio: ventanas emergentes, *banners*, cambios en la página de inicio o de búsqueda del navegador, etc. La publicidad está asociada a productos y/o servicios ofrecidos por los propios creadores o por terceros.

El *adware* puede ser instalado con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así. Lo mismo ocurre con el conocimiento o falta del mismo acerca de sus funciones.

### **Dialer**

Es un programa que, sin el consentimiento del usuario, cuelga la conexión telefónica que se está utilizando en ese momento (la que permite el acceso a Internet, mediante el marcado de un determinado número de teléfono) y establece otra, marcando un número de teléfono de tarificación especial. Esto supondrá un notable aumento del importe en la factura telefónica.

**cookies** son pequeños archivos de texto que el navegador almacena en el ordenador del usuario, cuando se visitan páginas web.

Las *cookies* almacenan información que se utiliza con varios fines:

Para personalizar la página web y su navegación para cada usuario.

Para realizar un seguimiento de qué *banners* se muestran al usuario, y durante cuánto tiempo.

Estos usos no tienen un carácter malicioso, al menos en principio.

Sin embargo, es necesario tener en cuenta que toda información personal que se introduzca en una página web se puede almacenar en una *cookie*, incluyendo el número de la tarjeta de crédito.

Además, las *cookies* también se pueden utilizar para formar un perfil del usuario, con información que éste no controla, y que después puede ser enviada a terceros, con la consiguiente amenaza para la privacidad.

**Pishing** es una forma de estafa bancaria, basada en el envío de mensajes electrónicos fraudulentos. Básicamente el "Pishing" es una forma de correo electrónico no solicitado, que pretende obtener información confidencial mediante la suplantación de las páginas de acceso a un servicio de banca electrónica.

Phishing es la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada. Normalmente se utiliza con fines delictivos duplicando páginas web de bancos conocidos y enviando indiscriminadamente correos para que se acceda a esta página y actualizar los datos de acceso al banco.

De forma más general, el nombre phishing también se aplica al acto de adquirir, de forma fraudulenta y a través de engaño, información personal como contraseñas o detalles de una tarjeta de crédito o cuentas bancarias (Usuario y Contraseña), haciéndose pasar por alguien digno de confianza con una necesidad verdadera de tal información (bancos, financieras, empresas de tarjetas de crédito) en un e-mail parecido al oficial, un mensaje instantáneo o cualquier otra forma de comunicación. Es una forma de ataque de la ingeniería social

### **¿Cómo funciona? ¿Cómo se distribuye?**

El mecanismo más habitualmente empleado es la generación de un correo electrónico falso que simule proceder de una determinada compañía, a cuyos clientes se pretende engañar. Dicho mensaje contendrá enlaces que apuntan a una o varias páginas web que replican en todo o en parte el aspecto y la funcionalidad de la empresa, de la que se espera que el receptor mantenga una relación comercial. Si el receptor del mensaje de correo efectivamente tiene esa relación con la empresa y confía en que el mensaje procede realmente de esta fuente, puede acabar introduciendo información sensible en un formulario falso ubicado en uno de esos sitios web.

## **WINZIP**

### **Introducción**

Es necesario saber cómo comprimir y descomprimir archivos a la hora de tener que adjuntarlos a los e-mails. De lo contrario, el proceso de enviar información como un "attach file" (archivo adjunto) sería muy lento y hasta complicado.

### **¿Para qué sirve?**

WinZip es una herramienta que trabaja con archivos comprimidos en formato ZIP. Este software se utiliza para comprimir y descomprimir archivos. Agrupa archivos en conjunto y los nombra como archivos con extensión ZIP.