**Tipos de virus de computadoras**  
  
  
**En informática, un virus de computadora es un programa malicioso desarrollado por   
programadores que infecta un sistema para realizar alguna acción determinada.   
Puede dañar el sistema de archivos, robar o secuestrar información o hacer   
copias de si mismo e intentar esparcirse a otras computadoras utilizando   
diversos medios. Siguiendo este link, podrás saber cómo un virus infecta a un   
sistema.**  
  
**Virus de Boot**  
  
**Uno de los primeros tipos de virus   
conocido, el virus de boot infecta la partición de inicialización del sistema   
operativo. El virus se activa cuando la computadora es encendida y el sistema   
operativo se carga.**  
  
  
**Time  Bomb o Bomba de Tiempo**  
  
**Los  virus del tipo "bomba de tiempo" son programados para que se activen en   
determinados momentos, definido por su creador. Una vez infectado un determinado   
sistema, el virus solamente se activará y causará algún tipo de daño el día o el   
instante previamente definido. Algunos virus se hicieron famosos, como el   
"Viernes 13" y el "Michelangelo".**  
  
  
**Lombrices,  worm o gusanos**  
  
**Con el interés de hacer un virus pueda  
  esparcirse de la forma más amplia posible, sus creadores a veces, dejaron de  
  lado el hecho de dañar el sistema de los usuarios infectados y pasaron a  
  programar sus virus de forma que sólo se repliquen, sin el objetivo de causar  
  graves daños al sistema. De esta forma, sus autores tratan de hacer sus  
  creaciones más conocidas en internet. Este tipo de virus pasó a ser llamado  
  gusano o worm. Son cada vez más perfectos, hay una versión que al atacar la  
  computadora, no sólo se replica, sino que también se propaga por internet   
enviándose a los e-mail que están registrados en el cliente de e-mail,   
infectando las computadoras que abran aquel e-mail, reiniciando el ciclo.**  
  
**Troyanos  o caballos de Troya**  
  
**Ciertos virus traen en su interior un   
código aparte, que le permite a una persona acceder a la computadora infectada o  
 recolectar datos y enviarlos por Internet a un desconocido, sin que el usuario  
 se de cuenta de esto. Estos códigos son denominados Troyanos o caballos de  
 Troya.**  
  
**Inicialmente,   
los caballos de Troya permitían que la computadora infectada pudiera recibir  
 comandos externos, sin el conocimiento del usuario. De esta forma el invasor  
 podría leer, copiar, borrar y alterar datos del sistema. Actualmente los  
 caballos de Troya buscan robar datos confidenciales del usuario, como  
 contraseñas bancarias.**  
  
  
**Los virus eran en el pasado, los mayores  
  responsables por la instalación de los caballos de Troya, como parte de su  
  acción, pues ellos no tienen la capacidad de replicarse. Actualmente, los  
  caballos de Troya ya no llegan exclusivamente transportados por virus, ahora  
  son instalados cuando el usuario baja un archivo de Internet y lo ejecuta.  
  Práctica eficaz debido a la enorme cantidad de e-mails fraudulentos que llegan  
  a los buzones de los usuarios. Tales e-mails contienen una dirección en la web  
  para que la víctima baje, sin saber, el caballo de Troya, en vez del archivo  
  que el mensaje dice que es. Esta práctica se denomina phishing, expresión  
  derivada del verbo to fish, "pescar" en inglés. Actualmente, la mayoría de los   
caballos de Troya simulan webs bancarias, "pescando" la contraseña tecleada por   
los usuarios de las computadoras infectadas. Existen distintas formas para saber   
si estás infectado con un troyano y cómo eliminarlo de tu   
PC.**  
  
**Hijackers**  
**Los  hijackers son programas o scripts que "secuestran" navegadores de Internet,  
  principalmente el Internet Explorer. Cuando eso pasa, el hijacker altera la  
  página inicial del navegador e impide al usuario cambiarla, muestra publicidad  
  en pop-ups o ventanas nuevas, instala barras de herramientas en el navegador y   
pueden impedir el acceso a determinadas webs (como webs de software antivírus,   
por ejemplo).**  
  
  
 **Keylogger**  
**El  KeyLogger es una de las especies de virus existentes, el significado de los   
términos en inglés que más se adapta al contexto sería: Capturador de teclas.   
Luego que son ejecutados, normalmente los keyloggers quedan escondidos en el   
sistema operativo, de manera que la víctima no tiene como saber que está siendo  
  monitorizada. Actualmente los keyloggers son desarrollados para medios  
  ilícitos, como por ejemplo robo de contraseñas bancarias. Son utilizados  
  también por usuarios con un poco más de conocimiento para poder obtener  
  contraseñas personales, como de cuentas de email, MSN, entre otros. Existen  
  tipos de keyloggers que capturan la pantalla de la víctima, de manera de saber,  
  quien implantó el keylogger, lo que la persona está haciendo en la computadora.  
  Cómo los keylogger nos roban la información? Cómo cuidarse?**  
  
**Zombie**  
**El  estado zombie en una computadora ocurre cuando es infectada y está siendo   
controlada por terceros. Pueden usarlo para diseminar virus, keyloggers, y   
procedimientos invasivos en general. Usualmente esta situación ocurre porque la   
computadora tiene su Firewall y/o sistema operativo desactualizado. Según   
estudios, una computadora que está en internet en esas condiciones tiene casi un   
50% de chances de convertirse en una máquina zombie, pasando a depender de quien   
la está controlando, casi siempre con fines criminales.**  
  
**Virus de Macro**  
  
**Los  virus de macro (o macro virus) vinculan sus acciones a modelos de documentos y a   
otros archivos de modo que, cuando una aplicación carga el archivo y ejecuta las  
 instrucciones contenidas en el archivo, las primeras instrucciones ejecutadas  
 serán las del virus.**  
 **Los virus de macro son parecidos a otros   
virus en varios aspectos: son códigos escritos para que, bajo ciertas   
condiciones, este código se "reproduzca", haciendo una copia de él mismo. Como  
  otros virus, pueden ser desarrollados para causar daños, presentar un mensaje o  
  hacer cualquier cosa que un programa pueda hacer.**  
**Nuevos medios**  
  
**Mucho se habla de prevención contra virus informáticos en computadoras personales, la   
famosa PC, pero poca gente sabe que con la evolución hoy existen muchos   
dispositivos que tienen acceso a internet, como teléfonos celulares, handhelds,   
teléfonos VOIP, etc. Hay virus que pueden estar atacando y perjudicando la   
performance de estos dispositivos en cuestión. Por el momento son casos   
aislados, pero el temor entre los especialistas en seguridad digital es que con   
la propagación de una inmensa cantidad de dispositivos con acceso a internet,   
los hackers se van a empezar a interesar cada vez más por atacar a estos nuevos   
medios de acceso a internet. También se vio recientemente que los virus pueden   
llegar a productos electrónicos defectuosos, como pasó recientemente con iPODS   
de Apple, que traían un "inofensivo" virus (cualquier antivirus lo elimina,   
antes de que él elimine algunos archivos contenidos en el iPod).**  
  
  
**Los más terribles: Los virus informáticos más famosos de la historia**  
**El primero: Cuál fue el primer virus informático?**  
  
  
 **Cómo remover un virus**  
  
**Guía básica para eliminar virus de una PC**  
  
**Muchos   
de nosotros alguna vez hemos sido victimas de algún virus que se haya alojado en   
nuestra PC, ocasionándonos más de un problema. Es por ello que a continuación se   
les enseñará a eliminarlo de manera simple y sin mayores dificultades. Es  
importante rescatar que para proceder a la eliminación definitiva de un virus  
 no siempre funcionará con la guía a presentar ya que un virus podría tener  
 distintas soluciones.**  
  
  
 **Primer paso:   
Diagnostico del PC.**  
  
**Si sospechas o este completamente seguro de que un virus ha sido alojado en tu PC,   
debido a que has notado algunos síntomas en el   
como:**  
  
**-Se reinicia continuamente**  
 **-El sistema operativo demora mucho en alzar**  
  
 **-Si el disco duro reporta falla**  
  
 **-Aparecen extensiones desconocidas**  
  
  
**El primer paso después de detectado el virus, es revisar el antivirus que cuentas   
actualmente instalado en tu PC, sino lo tienes es recomendable instales uno (es   
mejor tener solamente un antivirus instalado ya que al tener mas de uno podría   
causar conflictos en tu PC).**  
  
  
**Algunos nombres de los antivirus más conocidos son: Kaspersky, Avira Premium,   
BitDefender, ESET NOD32, Panda, Zone alarm.**  
  
  
**Segundo paso:   
Eliminar Virus.**  
  
**El segundo paso para eliminar el virus es desactivar el restaurador de sistemas por   
lo que existen algunos virus que son capaces de restaurarse inmediatamente   
después de cada reinicio de la PC, para esto deben dar clic derecho a las   
propiedades de MI PC y marcar la casilla de desactivar restaurar sistema o   
desactivar restaurar sistema en todas la unidades. Después de haber seguido los   
pasos anteriores se deberá reiniciar la PC pero ahora en modo a prueba de fallos  
(Apretando la tecla superior F8 al momento que esta alzando el sistema  
 operativo) después de esto debemos pasar el   
antivirus.**  
  
  
**Tercer paso:   
Verificando la eliminación del virus.**  
  
**Si realizó todos los pasos anteriores y su PC ya no presenta ningún síntoma de que   
aún se encuentre infectada, de ahora en adelante lo más recomendable es que  
diariamente pase el antivirus a su PC para así reducir el riesgo de que otro  
virus infecte a su PC.**  
  
**Además si desea limpiar continuamente su PC, un buen programa para ellos es el Ccleaner   
y no olvidarse sobre todo de tener actualizado su   
antivirus.**  
  
  
 **El seguir los pasos anteriormente mencionados hará que su PC se encuentre libre de   
virus o al menos este preparada por si uno de estos la   
infecta.**  
  
 **Seguridad y métodos de protección**  
Existen numerosos medios para combatir el problema; Sin   
embargo, a medida que nuevos programas y sistemas operativos se introducen en el   
mercado, más difícil es tener controlados a todos y más sencillo va a ser que a   
alguien se le ocurran nuevas formas de infectar sistemas. Los métodos para   
contener o reducir los riesgos asociados a los virus pueden ser los denominados   
activos o pasivos.  
  
  
Tipos de vacunas  
**Sólo detección**: Son  
 vacunas que sólo actualizan archivos infectados sin embargo no pueden  
 eliminarlos o desinfectarlos.  
  
**Detección y desinfección**: son   
vacunas que detectan archivos infectados y que pueden   
desinfectarlos.  
  
**Detección y aborto de la acción**: son   
vacunas que detectan archivos infectados y detienen las acciones que causa el   
virus  
  
**Comparación por firmas**: son   
vacunas que comparan las firmas de archivos sospechosos para saber si están   
infectados.  
  
**Comparación de firmas de archivo**: son   
vacunas que comparan las firmas de los atributos guardados en tu   
equipo.  
  
 **Por métodos**[heurísticos](http://es.wikipedia.org/wiki/Heur%C3%ADsticos):   
son vacunas que usan métodos heurísticos para comparar   
archivos.  
  
 **Invocado por el usuario**: son   
vacunas que se activan instantáneamente con el  
  usuario.  
  
 **Invocado por la actividad del sistema**: son vacunas que se activan instantáneamente   
por la actividad del sistema  
  operativo