# Lección 1.7

## Origen de los virus

A finales de la década de los 50 del siglo pasado, un curioso pasatiempo se puso de moda en los laboratorios Bell. Éste sólo podía ser disfrutado por un grupo de expertos en programación y fue bautizado con el nombre de **corewars** o guerras de núcleo, aunque también se le conoce como guerra de memoria.

El juego consistía en que cada jugador había de diseñar un programa que fuese capaz de reproducirse a sí mismo en el interior de la memoria de la computadora, y a la vez pudiese "devorar" las instrucciones de los demás jugadores. Al finalizar la jornada de trabajo, los jugadores colocaban sus programas en la memoria de la computadora (en la memoria RAM), en posiciones ocultas y ninguno de ellos sabía en qué ubicación se encontraba el otro, y procedían a activarlos, se daba a la computadora un tiempo previamente acordado, y a continuación se suspendía la ejecución y se examinaba la memoria. Aquel programa que resultara más abundante era el ganador.

La guerra de memoria fue inspirada en un programa escrito en lenguaje ensamblador llamado **Creeper**, el cual podía duplicarse cada vez que éste corría. Para contrarrestarlo fue creado el programa **Repeer**, cuya función fue la de destruir cada copia hecha por creeper, y autodestruirse cuando ya no existiera ningún creeper.

Uno de los métodos más seguros para evitar la contaminación por virus es desconectar y guardar la computadora.

Los jugadores de este juego, acordaron no revelar nunca al público los detalles de sus juegos sin embargo en 1983 este código de honor de los programadores fue roto. El culpable fue Ken Thompson, el hábil ingeniero de software que escribió la versión original del sistema operativo UNIX.

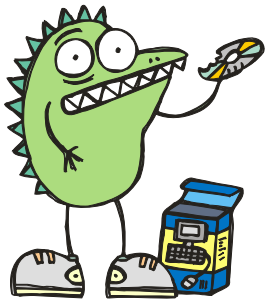
Thompson se presentó a la Asociación para Maquinaria de la Computación y dio un discurso que no solamente revelaba la existencia de los primeros virus computacionales, sino mostró a la audiencia cómo hacerlos y los invitó a crearlos.

La revelación fue publicada en el artículo "Dewdeny", en mayo de 1984, en la edición de "Scientific American", en el cual describió la "Guerra de Memoria", e invitó a los lectores a que enviaran dos dólares por correo por una copia de las guías para crear sus propios campos de batallas virales.

# Síntomas y consecuencias de contaminación

Hoy en día es muy importante conocer y saber lo que un determinado virus podría provocar en la computadora, los CD y las memorias flash, por lo que es de vital importancia conocer sus efectos:

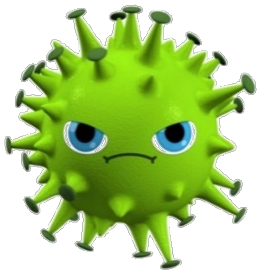
- De repente la computadora ya no reconoce a la memoria flash.
- Se lleva más tiempo de lo normal la carga de un programa.
- Marcan áreas dañadas del disco duro, cuando éstas ni siquiera han sido utilizadas, disminuyendo su capacidad.



- Infectan el sistema operativo.
- Provocan imágenes molestas o envían mensajes en el monitor.
- Borran programas o archivos.
- Dañan físicamente a la computadora, aumentando el acceso a sectores de disco y el uso de las cabezas de lectura causan un daño prematuro por uso excesivo, o provocan su caída sobre el disco, causando daños fatales.
- Llenan de basura la memoria de la computadora.

- Impiden el acceso a Internet.
- Reinicializan la computadora (CTRL+ALT+DEL) de repente.
- Bloquean el teclado.
- Modifican la información en programas o archivos.
- Y cualquier otra acción que se les ocurra a los creadores.

# Clasificación de virus



"No compre una computadora". 1ª Ley de Richarson de la seguridad informática.

"Si compra una computadora, no la encienda". 2ª Ley de Richarson de la seguridad informática.

Como habíamos mencionado anteriormente, las computadoras pueden enfermarse al igual que las personas. De una computadora a otra puede propasarse gran variedad de enfermedades muy contagiosas, en forma muy similar a como los virus biológicos se difunden entre los humanos. Un virus de computadora es un programa que literalmente "infecta" a otros programas y bases de datos con su contacto. También puede ocultar réplicas de sí mismo dentro de programas legítimos, por ejemplo, un sistema operativo o un procesador de textos. Estos virus residen en los CD y memorias flash y se transmiten a través de ellos.

Existen muchos tipos de virus. Algunos actúan rápidamente y borran programas y datos del usuario en el disco, otros crecen como un tumor destruyendo pequeñas partes de un archivo cada día. Otros más actúan como bomba de tiempo, pues están latentes durante días o meses, pero llega el momento en que se activan y causan un desastre en cualquier programa del sistema.

Aunque no existe una clasificación general exacta de los virus, ya que varía de publicación en publicación del tema, podemos agruparlos de la siguiente manera:

Cuando tenemos una computadora, no falta que nos encontremos por ahí un programa muy apetitoso para llevarlo a casa.

¡Cuidado, puede tratarse de un virus! Di no a la piratería.

I. **Caballos de Troya**, vienen escondidos en el interior de un juego, o de una versión de demostración de un software muy llamativo. El usuario se trae el software con intención de probarlo y en principio no nota la diferencia con un programa correcto. Sin embargo al ejecutar el programa, este, de modo oculto al usuario, estaría realizando otro tipo de acciones tales como borrar código, enviar copias de información por la red, etc.

II. **Bombas de tiempo**, se activan en determinadas fechas o tras una serie determinada de ejecuciones, o bien si un usuario no paga un programa legal se activa el virus.

III. **Replicador**, son parecidos a los virus biológicos, ya que se autorreproducen e infectan a los archivos ejecutables.

IV. **Gusanos o worms**, examinan la cantidad de información almacenada, y si es muy poca se esperan, y cuando ha llegado a 50% proceden a borrarla, marcan sectores dañados del disco disminuyendo su capacidad de almacenamiento y se llaman gusanos porque literalmente se arrastran en la red de computadora en computadora.

V. **De macros / código fuente**, se hacen pasar por macros de documentos de texto u hojas de cálculo, al ser ejecutada la macro donde se esconden, se activa el virus.

VI. **Mutantes o polifórmicos**, van modificando su código para no ser detectados por las vacunas.

VII. **Infectores de programas ejecutables**, son los más peligrosos, ya que se diseminan fácilmente (en hojas de cálculo, base de datos, etc.), saturan la capacidad de almacenamiento y se activan al ejecutar el programa que lo tiene infectado.

## Formas de contagio

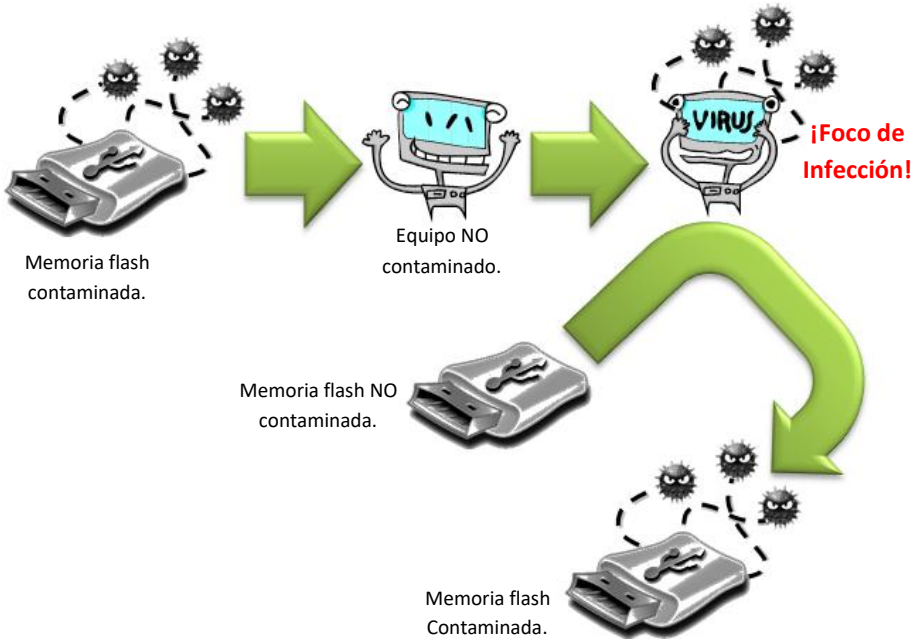
Existen tres fuentes básicas de contagio de virus:

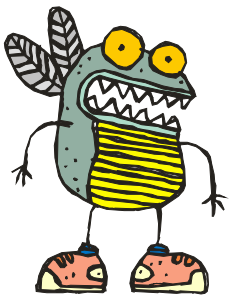
Si tenemos una memoria flash contaminada, y la introducimos a una computadora no contaminada, ésta se contamina si no tomamos medidas de prevención, en este momento la computadora queda infectada y se convierte en un foco de infección, ya que cualquier memoria que sea introducida en ella, quedará contaminada sin remedio. A esto se le llama ciclo de los virus. Cabe mencionar que una memoria o un equipo contaminado puede contener varios tipos de virus al mismo tiempo.

### 1.-Por medio de memorias flash

Los virus se propagan de un sistema a otro a través de las memorias flash, las cuales son uno de los vectores de contagio más común, ya que al introducir nuestra memoria en una computadora para extraer información, si ésta se encuentra contaminada inminentemente la memoria queda contaminada y al introducirla en nuestra computadora también la contaminamos.

En las escuelas pasa lo siguiente, un estudiante con una memoria infectada puede contagiar sin saberlo a varias computadoras del laboratorio; a su vez, el virus contagia a las memorias de otros estudiantes.



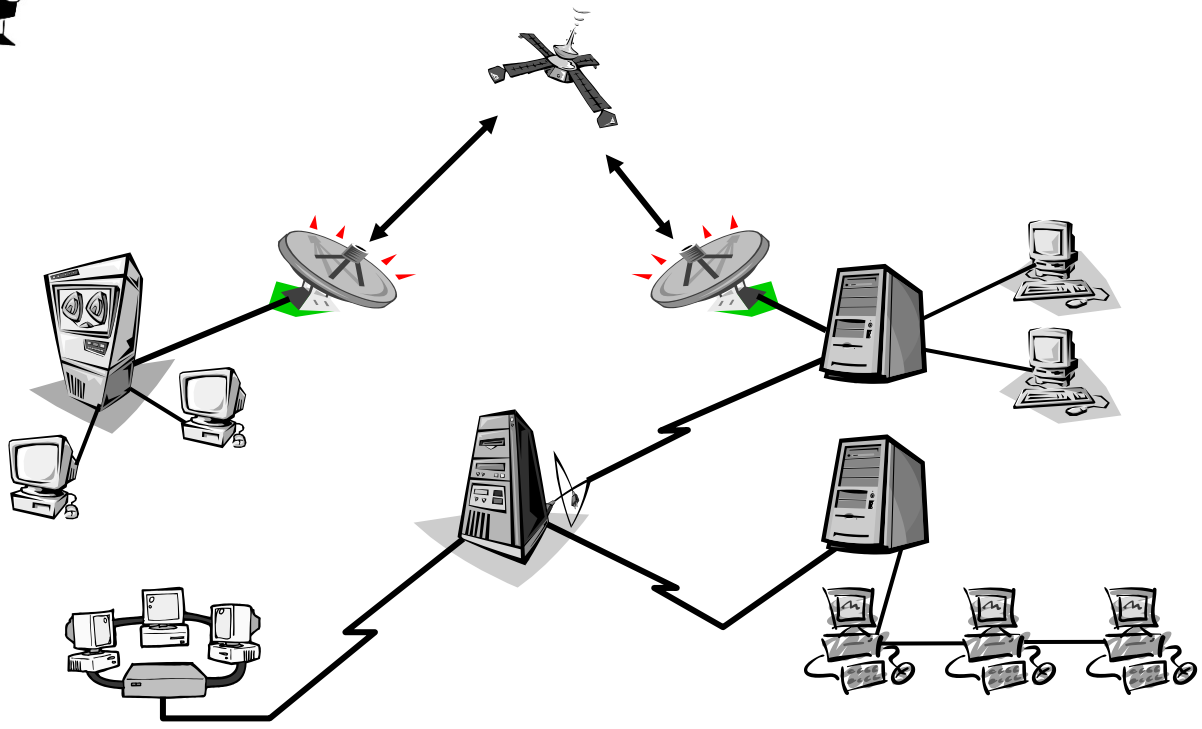
## 2.-Acceso a Internet

Con el acceso a Internet, los usuarios de computadoras personales, hemos tenido muchas ventajas, acceder a información reciente de cualquier tema y bajarlo a nuestra computadora, copiar software gratis que ofrece la red, hacer amigos nacionales e internacionales mediante las redes sociales como Facebook, acceder a educación virtual, acelera el envío de información mediante correo electrónico, hacer pagos o transferencias bancarias desde casa, etc. La fuente más común de infección por virus son los boletines electrónicos públicos, en los que los usuarios intercambiamos software. Por lo general, al conectarnos al boletín y bajar lo que pensamos que es un juego, un programa de utilerías o cualquier otro tentador programa, podemos recibir un virus.

## 3.-Redes de cómputo


A reserva que este tema lo veamos con mayor detenimiento en el capítulo de Internet, podemos decir que una red de cómputo es la conexión de varias computadoras, que tienen como objetivo compartir recursos, tales como programas, archivos o carpetas, impresoras, etc. Los virus pueden pasarse de una computadora a otra en una red o bien de una red a otra.

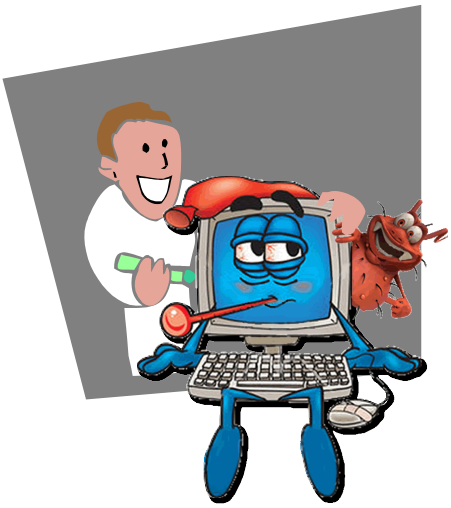
Los usuarios de red estamos expuestos frecuentemente a contagio viral, por eso las normas de seguridad e higiene computacionales deben ser muy estrictas.



# Medidas preventivas y correctivas

Cuando bajamos información de Internet, hay muchas probabilidades de traernos virus.

- Tener instalado un programa antivirus original.
- Antes de intercambiar información de una memoria flash, verificar que esté limpia mediante un antivirus.
- Permitir únicamente la incorporación de programas originales.
- No utilizar copias ilegales de ningún producto.
- Mantener los discos originales (programas, utilerías, lenguajes, etc.) en lugares seguros y trabajar con copias de respaldo que se hayan hecho de ellos.
- Controlar el acceso al uso de las computadoras.
- No hacer uso de una computadora que esté encendida, sin antes preguntar si tiene instalado un antivirus.
- Guardar un respaldo “sano” y protegido del sistema operativo.
- Mantener respaldo de la información valiosa.
- En la medida de lo posible, no prestar memorias flash.



La mejor forma de tratar con los virus es reconocer su existencia y tomar medidas preventivas. Las posibilidades de vivir sanos de virus aumentan en gran medida si se revisa periódicamente (se ejecuta un programa antivirus) y se tiene cuidado con lo que se carga en el disco duro del sistema.

Muchas compañías recomiendan a sus usuarios de PC que respalden todo el software antes de cualquier día viernes trece, fecha favorita de quienes crean los programas de virus. Algunos de éstos atacan el hardware y se ha sabido de casos en los que causan costosos espasmos a componentes mecánicos del sistema, como los brazos de acceso a disco.

**Antivirus**: son programas hechos para detectar y eliminar a los virus de las computadoras, también se les conoce como **vacunas**, y dado el incremento de virus existentes siempre hay más virus que vacunas.

## Antivirus

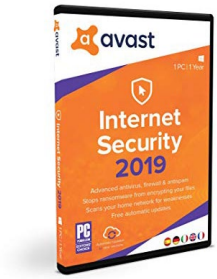
Así como los virus computacionales son programas creados por el hombre para destruir información o poner en jacke a un sistema de cómputo, las vacunas o antivirus son otros programas para contrarrestar a los primeros.

Hoy en día, y debido a la gran proliferación de virus, existen varias compañías que se dedican a la detección de virus, su captura y el desarrollo de vacunas.

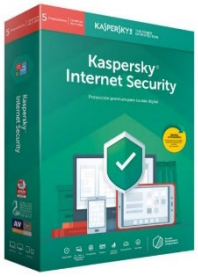
Las vacunas o antivirus nos ayudan a proteger todo nuestro sistema desde un único programa y realizar análisis en busca de virus. Cuando queramos y desde la misma pantalla, podemos rastrear y vacunar los archivos de la computadora, el correo electrónico y las memorias Flash.

Algunas vacunas permiten analizar los mensajes de correo y protegerse de los que llegan o se envían, en cualquier momento y sin que sea necesario abrir el antivirus.

Las compañías de vacunas o antivirus ofrecen:




Avast! Antivirus.




Kaspersky Antivirus.

- Actualizaciones diarias o frecuentes del archivo de firmas de los virus en forma automática a través de Internet, esta es la forma más sencilla y rápida para mantener la protección antivirus actualizada diariamente.
- Soluciones completas y globales que, además de detectar los virus, proporcionan todos los medios y servicios necesarios para eliminarlos y para ayudarnos siempre que lo necesitemos.
- Soporte Técnico On-Line, servicio por el que, rápida y fácilmente, vía e-mail, podemos plantear nuestras consultas a los técnicos calificados de la compañía, que resuelven las 24 horas de los 365 días del año, cualquier problema que tengamos relacionado con el funcionamiento del programa antivirus.
- Ayuda las 24 horas, servicio por el que la gran mayoría de las compañías se comprometen a analizar cualquier archivo que sospechemos que está infectado y respondernos, en menos de 24 horas, con una solución, aunque el virus sea nuevo y desconocido. Con el objetivo de responder oportuna y eficientemente ante este tipo de incidencias.

La mejor compañía de antivirus es aquella con la que el usuario se sienta más seguro y satisfecho de su servicio. Si somos usuarios nuevos, antes de comprar un antivirus conviene checar todas aquellas marcas en el mercado, y elegir la que más se ajuste a nuestras necesidades y presupuesto.

# Muro de fuego

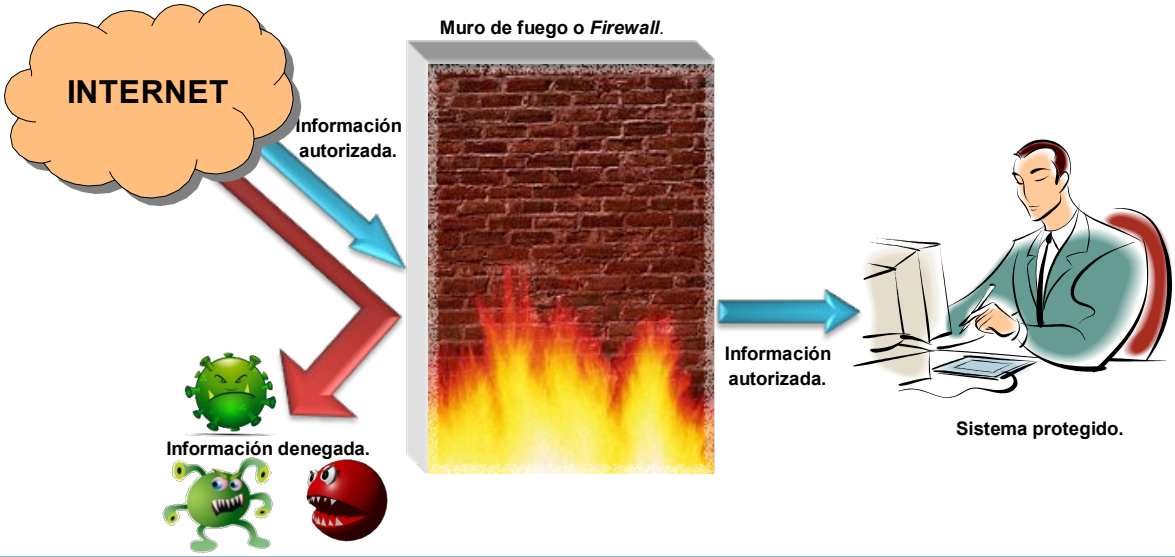
Un Muro de fuego o *Firewall*, es una protección para los usuarios que nos conectamos a Internet. El *Firewall* revisa y verifica las actividades de nuestra computadora al estar conectada a Internet, por ejemplo, el Muro de fuego revisa los programas que están abiertos, quién se conecta a nuestra máquina vía Internet, ya que verifica la autenticidad del usuario que se conecta con nosotros y si está autorizado le permite el acceso.

Como podemos ver, es un sistema básico de seguridad que debemos utilizar para nuestra conexión a Internet, pero también si trabajamos en red, ya que un *Firewall* es un sistema de defensa que se basa en la instalación de una "barrera" entre nuestra PC y la red, por la que circulan todos los datos. El tráfico entre la red y nuestra PC es autorizado o denegado por el Muro de fuego (la "barrera"), siguiendo las instrucciones que le hayamos configurado.

Un Muro de fuego funciona, en principio, DENEGANDO cualquier tráfico que se produzca cerrando todos los puertos de nuestra PC. En el momento que un determinado servicio o programa intente acceder a nuestra PC nos lo hará saber, podremos en ese momento aceptar o denegar dicho tráfico, pudiendo asimismo hacer (para no tener que repetir la operación cada vez) "permanente" la respuesta hasta que no cambiemos nuestra política de aceptación.

**Windows 10** incluye un *Firewall* bastante bueno, potente y muy configurable, que se encuentra en **Actualización y seguridad** de **Configuración de Windows**.

Ahora bien, es muy importante mencionar que el *Firewall* no es un antivirus, es un sistema complementario, por lo que es indispensable tener instalado también un antivirus en nuestra computadora, y así estar protegidos perfectamente contra amenazas virales o personas ajenas cuando navegamos por Internet.



# Hacker-Cracker

## Hacker

Hacker.

Un **hacker** (del inglés *hack*, recortar) se utiliza para referirse a un experto en varias o algunas ramas relacionadas con la computación y telecomunicaciones, tales como: programación, redes de comunicaciones, sistemas operativos, hardware de red y voz.

La palabra **hack** (recortar) es utilizada en determinados sectores de la tecnología para denominar a las pequeñas modificaciones que se le pueden hacer a un programa o máquina, para mejorar o alterar su funcionamiento.

Se dice que el término hacker surgió de los programadores del Massachusetts Institute of Technology (MIT), que en los años 60 del siglo pasado, por usar hacks se llamaron a sí mismos hackers, para indicar que podían hacer programas mejores y más eficaces, o que hacían cosas que nadie había podido lograr.

En el mismo sentido, se suele decir que el sistema Linux fue creado por el hacker Linus Torvalds y dio el nombre a este sistema al mezclar su primer nombre con el del sistema operativo Unix.

Ahora bien, a las obras propias de un hacker, se le llama hackeo y hackear.

La descripción más pura de un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y/o compartirlas sin limitaciones con los demás.

El término actualmente es algo ambiguo, ya que también se utiliza para referirse a:

- Aficionados a la informática que buscan defectos, puertas traseras y mejorar la seguridad del software, así como prevenir posibles errores en el futuro.
- Delincuentes informáticos, o crackers, y que sería incorrecto según los propios hackers.

## Cracker

Cracker.

Un **cracker** (del inglés *crack*, romper) es alguien que viola la seguridad de un sistema informático con fines de beneficio personal o por mera diversión, también se le conoce como pirata informático. Asimismo se considera como cracker a aquella persona que diseña y programa cracks informáticos.

El término fue creado alrededor de 1985 por los hackers, como defensa por el uso incorrecto del término hacker. Se considera que la actividad del cracker es ilegal.

En otras palabras, son cibervándalos que aplican sus vastos conocimientos de programación e informática para eliminar la seguridad de programas, juegos, etc.

Para prevenir estas intromisiones indeseables a nuestra computadora, el *Firewall* es un arma importante, aunque también podemos adquirir programas especializados en el combate de los cracker, aun cuando muchos productos digan anti-hacker, debemos estar conscientes que en realidad es para contrarrestar los ataques de los cracker.