

APÉNDICE A Virus informáticos

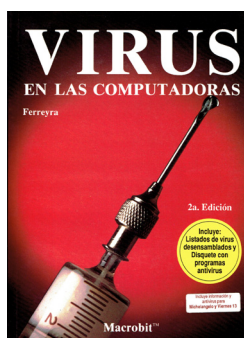
Los virus informáticos se propagan en las computadoras autocopiándose en los medios de almacenamiento de la información y en la memoria RAM. Algunos entran al sistema con una imagen aparente, diferente a su cometido, y cuando menos te lo esperas, comienzan a reproducirse y a presentar comportamientos extraños y molestos.

A este tipo de virus se le conoce como **Trojanos**, en recuerdo de la anécdota del **Caballo de Troya** de la mitología griega. Protege tu información haciendo lo siguiente:

- Realiza copias de seguridad de todos tus archivos de texto, hojas de cálculo, presentaciones, bases de datos, imágenes y música.
- Utiliza las **Herramientas de sistema** de Windows para hacer mantenimiento preventivo del sistema y de los discos de almacenamiento.
- Instala un antivirus y mantenlo actualizado diariamente a través de Internet para proteger tu información de ataques de virus y programas de **malware**.



A.1 Los virus de las computadoras



Uno de los primeros libros sobre virus informáticos en México.

“hace pocos años nadie hubiera imaginado que su computadora podría enfermar... presentar síntomas desconocidos... y mucho menos que esta enfermedad fuera causada por... ¡un mortífero virus!”

Gonzalo Ferreyra Cortés
Virus en las computadoras, Alfaomega, 1990.



Definición de virus

Los virus informáticos no son más que programas, ¡sí, programas de computación elaborados por programadores!, archivos que contienen instrucciones para que las ejecute la computadora. Los virus de computadoras sólo realizan las tareas que fueron programadas en su código, ¡ni más, ni menos!

Así como hay programas para las diferentes plataformas de computadoras, también se crean virus para cada una de ellas. Hay más virus para las PC con Windows, pero eso es lógico, ya que más del 90% de las computadoras de todo el mundo utilizan ese sistema operativo.

Están escritos generalmente en lenguaje de máquina, en ensamblador o en cualquier lenguaje de programación, y tienen algunas características especiales, de donde se puede partir a hacer una definición completa de ellos:

1. Son muy pequeños, lo que los hace difíciles de detectar y eliminar.
2. Se auto reproducen en la memoria de la computadora o en las unidades de almacenamiento de datos.
3. Casi nunca incluyen en el código, ni nombre de autor, ni copyright, ni fecha de creación.
4. Al ejecutarse toman el control de la computadora y modifican otros programas.
5. Ralentizan el funcionamiento de la computadora.
6. Tienen la capacidad de “escondarse” para no ser descubiertos, mutando su forma, o utilizando técnicas llamadas “*Stealth*”.
7. Pueden sólo causar molestias al usuario, u ocasionar graves daños a los datos almacenados en las unidades de la computadora.

Desde antes de 1990 el problema de los virus informáticos se extendía en el cada vez más creciente número de computadoras PC. Para contrarrestar a los virus se creó la **Computer Virus Industry Association**, CVIA, comandada entonces por **John McAfee** (1945-), en donde se detectaron más de 500 programas virales, que ya habían infectado a unas 200,000 computadoras sólo en Estados Unidos. Actualmente hay informes confiables que hablan de más de un millón de virus, aunque los activos no pasen de unos cuantos miles.

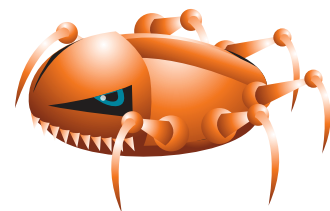


DEFINICIÓN

Un virus informático es un programa que se ejecuta sin el consentimiento del usuario: al ser ejecutado altera el correcto funcionamiento del sistema; puede insertar copias de sí mismo en otros programas o áreas de los discos; destruye programas o datos en la memoria RAM, o en unidades de almacenamiento; marca los programas infectados para reconocer que ya han sido modificados, y se reproduce de manera infinita en la memoria y en los medios de almacenamiento.

Cómo funcionan los virus informáticos

Como todos los programas, los virus informáticos necesitan que alguien los ejecute en la computadora para que realicen las tareas para las que fueron programados. De ninguna manera se pueden ejecutar solos. Al ejecutar un programa infectado, se cargan en la memoria RAM y permanecen ahí mientras se mantenga encendida la computadora. Algunos se cargan al ejecutar un programa infectado que llegó como archivo adjunto en un correo electrónico.

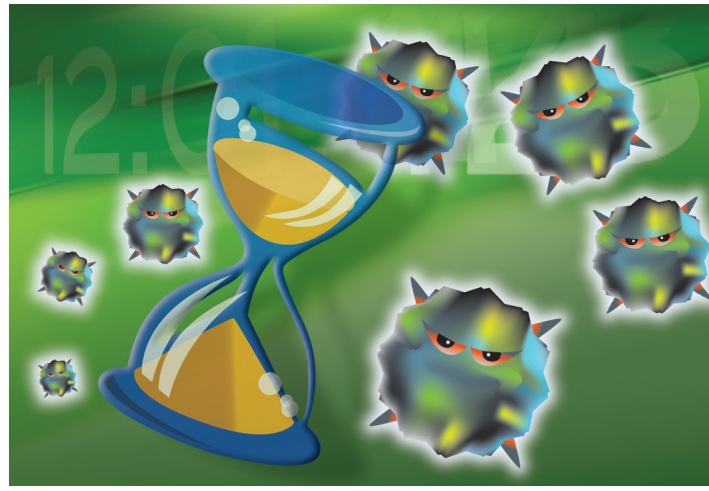


Nota: Otra forma de infección se da cuando se deja un disco infectado del área de carga, en la unidad de CD-ROM, DVD o USB. Al encender o reiniciar la computadora, en lugar de ejecutarse el programa de carga primero, el virus busca alojarse en la memoria RAM e infectar el área de carga o la tabla de particiones del disco duro.

El virus puede actuar de inmediato, o esperar a que se den las condiciones o señales propicias que fueron programadas en su codificación. Al entrar en acción, el virus informático toma el control de la computadora desde el principio y a partir de ese momento, cualquier disco o unidad de almacenamiento que se inserte, quedará infectado al realizar cualquier acceso de lectura o escritura.

Busca infectar de inmediato alguna de las áreas críticas de los discos como el área de carga, la **tabla de particiones**, la **tabla de asignación de archivos**, el **directorio raíz**; o algún archivo ejecutable con extensión **.com**, **.exe**, **.dll**, **.bat**, **.ovr**, o cualquier otro.

Algunos comienzan su acción destructora de inmediato, otros esperan a que se den ciertas condiciones que se han incluido en su código, como una fecha y hora; la ejecución de alguna orden, o la realización de algún evento específico. Por último, los hay que, en el momento de la infección, inician un contador que les indicará el momento de activarse. Otros virus conviven también como macros de documentos de Word, Excel, PowerPoint o correos electrónicos de cualquier tipo.



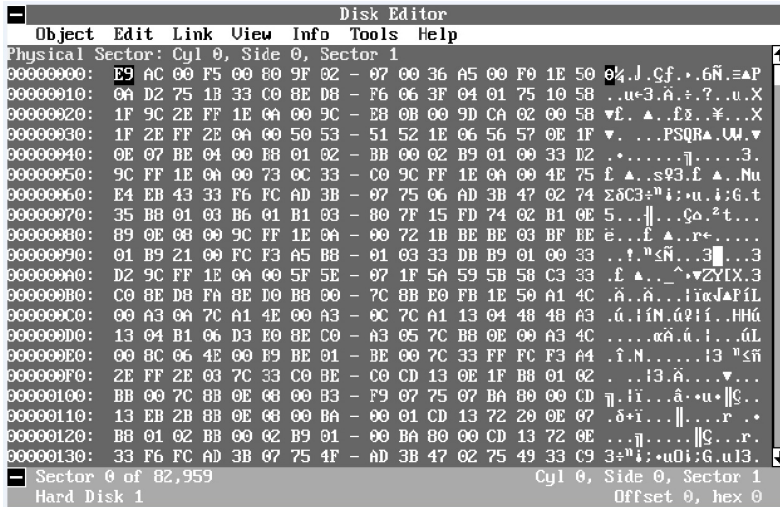
Los que infectan el **área de carga**, se posicionan en la memoria de la computadora desde el momento de encenderla, porque al iniciar, en lugar de leer el programa de carga, se lee primero el código del virus. Para no alertar a la computadora con un mal funcionamiento, el virus manda leer el programa de carga, que se encuentra en otro sector, donde lo envió el propio virus. De esta manera, el virus ya está en la memoria, y el usuario ni se entera, porque aparentemente no hay problemas.

```

Disk Editor
-----
Object Edit Link View Info Tools Help
Physical Sector: Cyl 0, Side 0, Sector 1
00000000: FA 33 C0 8E D0 EC 00 7C - 8B F4 50 07 50 1F FB FC B.ãð..iñP•Pv¹³
00000010: BF 00 06 B9 00 01 F2 A5 - EA 1D 06 00 00 BE BE 07 .....NÜ....¥¥*
00000020: B3 04 80 3C 80 74 0E B0 - 3C 00 75 1C 83 C6 10 FE .ç<çtç<.u.ää.■
00000030: CB 75 EF CD 18 8B 14 BB - 4C 02 8B EE 83 C6 10 FE .u..iñiL.i_ää.■
00000040: CB 74 1A 80 3C 00 74 F4 - BE BB 06 AC 3C 00 74 0B .t>ç<.tñi.¼<.td
00000050: 56 BB 07 00 B4 0E CD 10 - 5E EB F0 EB FE BF 05 00 Uñ..ñ..Ù-Uñ.ç.
00000060: BB 00 7C B8 01 02 57 CD - 13 5F 73 0C 33 C0 CD 13 ñ.Û..W.!_s93..!!
00000070: 4F 75 ED BE A8 06 EB D3 - BE CA 06 BF FE 7D 81 3D Du¥z.ÜE¥...ñü=
00000080: 55 AA 75 C7 8B F5 EA 00 - 7C 00 00 54 61 62 6C 61 U-uñiSÜ.l..Tabla
00000090: 20 64 65 20 70 61 72 74 - 69 63 69 A2 6E 20 6E 6F de partición no
000000A0: 20 76 A0 6C 69 64 61 00 - 45 72 72 6F 72 20 61 6C válida.Error al
000000B0: 20 63 61 72 67 61 72 20 - 73 69 73 74 65 6D 61 20 cargar sistema
000000C0: 6F 70 65 72 61 74 69 76 - 6F 00 46 61 6C 74 61 20 operativo.Falta
000000D0: 73 69 73 74 65 6D 61 20 - 6F 70 65 72 61 74 69 76 sistema operatiu
000000E0: 6F 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 o.....
000000F0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .....
00000100: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .....
00000110: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .....
00000120: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .....
00000130: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .....
Sector 0 of 499,454 Cyl 0, Side 0, Sector 1
Hard Disk 1 Offset 0, hex 0
    
```

Norton Editor versión 7.0 mostrando el sector 0 de un disco duro "sano".
 Observa que el primer valor hexadecimal es FA.

Nota: Cuando el virus **Michelangelo** infectaba un disco duro, la **tabla de particiones** o **Master Boot Record (MBR)** se desplazaba a la dirección física: **Cilindro 0, Lado 0, Sector 7**, y el virus se alojaba en el lugar del **MBR**. **Michelangelo** cabía en un sector, ya que su longitud era de sólo **429** bytes (los sectores contenían un total de **512**). Si el programa de carga inicial no está alojado en el área de carga inicial (**Boot sector**), puede suponerse que un virus lo ha desplazado a otro sector, y ha tomado su lugar en el sector de arranque.



El sector 0 del mismo disco cuando era infectado por el virus **Michelangelo**. Mira cómo el primer valor hexadecimal cambió a **E9**.

Clasificación de los virus de computadoras

Existen muchas clasificaciones de los virus informáticos. Cada compañía fabricante de **antivirus** y cada investigador hacen una clasificación que, desde su punto de vista, debe considerarse como la adecuada. Lo cierto es que los virus se pueden clasificar según diversos criterios.

De acuerdo con el área que infectan:

- **Infectores del área de carga inicial.** Infectan a las unidades de almacenamiento, alojándose en el área de carga, que se encuentra en el sector 0. Cambian de lugar al programa de carga, enviándolo a otro sector del disco. Desde el encendido de la computadora toman el control del sistema.
- **Infectores de sistema.** Infectan a los programas de sistema, que son de los primeros que se cargan en la memoria de la computadora, junto con el virus, obviamente.
- **Infectores de programas ejecutables.** Insertan una copia de sí mismos en el código de los programas ejecutables, que tienen extensiones **.com**, **.exe**, **.dll** y otros. Son muy peligrosos porque realizan una búsqueda de archivos ejecutables para infectarlos a todos; cuando estos archivos se desinfectan con un programa antivirus, generalmente quedan inservibles, por lo que hay que instalar nuevamente los programas y hasta restaurar el sistema operativo.



Los virus **burlones**, además de cometer sus fechorías en la computadora, se burlan del usuario.

- **Infectores de documentos.** Infectan a los documentos de Word, Excel y PowerPoint, alojándose en el área de **macros**. Infectan a todos los archivos que tienen las extensiones de los documentos de Office.

De acuerdo con su forma de operación

- **Caballos de Troya.** Programas que se introducen al sistema mostrando una apariencia diferente a la de su objetivo final. Muchos investigadores no consideran a los troyanos como virus, aunque la mayoría actúa como tales. Su nombre recuerda el episodio del **Caballo de Troya**, que permitió el rescate de **Helena** por las huestes de **Menelao**.
- **Gusanos.** Programas auto replicables, que se diseminan a través de las redes y en la memoria de las computadoras, sin la ayuda de un programa anfitrión ejecutable. Se arrastran literalmente por las áreas de la memoria borrando los datos de programas e información, produciendo fallas que parecieran ser del sistema.



Nota: Los gusanos (*Worms*) se cargan en la memoria de la computadora y se posicionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente, esto hace que se borren los programas o la información que se encuentren a su paso, causando problemas de operación o pérdida de datos.

- **Bombas de tiempo.** Son programas ocultos en la memoria del sistema, en algunas áreas de los discos o en programas ejecutables, que esperan una fecha y hora determinadas, para *explotar*; es decir, para comenzar con su actividad virulenta. Algunos no son destructivos, y sólo exhiben mensajes en la pantalla en el momento de la *explosión*, otros son bastante perjudiciales.
- **Auto-replicables.** Son los programas que realizan las funciones más parecidas a los virus biológicos, ya que se auto reproducen e infectan los programas ejecutables que encuentran en el disco. Se ejecutan en un determinado momento programado, cada determinado tiempo, al llegar un contador a su fin, o cuando “sienten” que se les trata de detectar.
- **Mutantes.** Programas que se ocultan y engañan a los antivirus modificando su código mediante esquemas de **encriptación** o **codificación**. Utilizan técnicas llamadas **sigilosas** (*Stealth*) o invisibles, para escabullirse de la vista de los antivirus.
- **Macrovirus.** Son macroinstrucciones de programas como Word, Excel o PowerPoint, que se reproducen en el sistema al abrir un documento infectado.

Antivirus. Programa que protege y ayuda a eliminar los virus informáticos que se introducen en las computadoras, rastreando la memoria y las unidades de almacenamiento.

Macros. Macroinstrucciones. Pequeños programas de tipo “script”, que realizan los usuarios de aplicaciones de oficina, para llevar a cabo tareas repetitivas relacionadas con procesadores de textos, hojas de cálculo, etc.

Encriptación. Codificación que se lleva a cabo en archivos, cambiando cadenas de caracteres por símbolos equivalentes, para evitar que sean entendidos por extraños. Para descifrarlos, se requiere de una contraseña.

- **Virus de correo electrónico o Internet.** Se introducen a las computadoras al acceder a páginas web que ofrecen archivos y programas gratuitos, o mediante el correo electrónico, como archivos adjuntos.
- **Secuestradores.** *Hijackers.* Los nuevos programas de *malware* actúan sobre las aplicaciones de redes e Internet, como los navegadores o los programas de mensajería instantánea, secuestrándolos literalmente. Cuando eso sucede, no puedes cambiar de página inicial, se presentan ventanas indeseables (*Pop-ups*) y se bloquean direcciones de páginas web de empresas de antivirus.
- **Caza contraseñas.** *KeyLoggers.* Programas que se introducen a las computadoras, residen en la memoria, y envían a sus creadores cada una de las pulsaciones que hace el usuario en el teclado. De esta manera, roban contraseñas y números de cuentas.
- **Espías.** *Spyware.* Programas que recopilan información importante acerca de la identidad de los usuarios, y de las actividades que realizan en la computadora, para crear bases de datos y venderlas a empresas que utilizan estos datos para llenar los buzones con **correo electrónico “basura” (Spam)**.
- **Esquemas de protección.** Código que puede ser dañino, introducido en algunos programas comerciales, que detectan si se realizan copias del disco original. Al cabo de algún tiempo, cuando se han creado bastantes archivos importantes, modifica su estructura y no permite que la computadora siga funcionando correctamente, lo que obliga al usuario a comprar el programa original para recuperarlos. Un ejemplo claro de este tipo de virus es el *Pakistán*, como verás más adelante.

A.2 Historia de los virus de computadoras

Debido al misterio que envolvió a estos dañinos programas durante muchos años, no existe ninguna información fidedigna que permita reconstruir con exactitud la historia de los virus informáticos y los contagios virales. Las empresas, institutos de investigación, agencias gubernamentales e instituciones educativas que ya habían padecido alguna infección por virus, lo negaban, para no reconocer que los sistemas de seguridad implantados resultaban vulnerables.

En 1949, **John von Neumann** (1903-1957), *Padre de la Computación*, describió algunos programas que se reproducen a sí mismos en su ponencia *Teoría de Automatas Auto reproductivos (Theory and Organization of Complicated Automata)*. Esto, aunque no se enfocaba a la creación de programas que se diseminan sin permiso de los usuarios de computadoras, si no es el comienzo de los virus, sí es el primer indicio de código autor reproductor.



John von Neumann, matemático húngaro nacionalizado estadounidense, fue discípulo de **Albert Einstein** (1879-1955) y pionero de la computación digital.

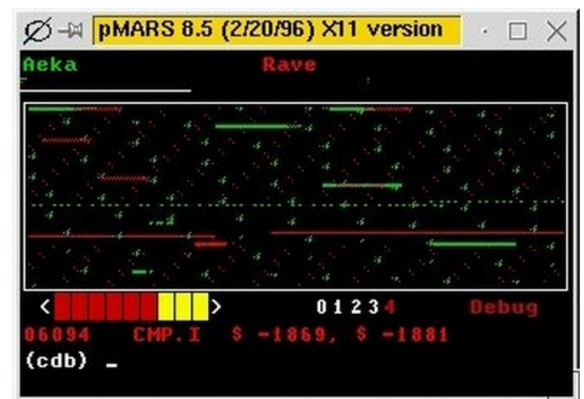
En la década de 1960, estudiantes de computación en el *Instituto Tecnológico de Massachusetts*, se reunían por las noches para elaborar **código sofisticado** de programas como **Guerra en el espacio** (*Spacewar*). Jugaban entre ellos bombardeando al programa contrincante. No eran propiamente virus, sino *bombas* que actuaban *explotando* al momento.



Spacewar está considerado como el primer juego interactivo de computadora. Fue desarrollado por **Steve Russell** (1937-) en el *MIT*. Reproducción de la computadora *PDP-1* y del programa, en el museo de historia de la computación en Mountain View, California.

En 1972, varios científicos estadounidenses de los laboratorios de computación de la AT&T (*Bell Laboratories*): **H. Douglas Mellory**, **Robert Thomas Morris Sr.** (1932-2011), **Victor Vysotsky** y **Ken Thompson** (1943-), *ingeniero en sistemas*, creador de la primera versión del sistema **Unix**, para entretenerse inventaron el juego **Guerra nuclear** (*CoreWar*), inspirados en un programa escrito en lenguaje ensamblador llamado **Creeper**, el cual tenía la capacidad de reproducirse cada vez que se ejecutaba.

El juego **Guerra nuclear** consistía en invadir la computadora del adversario con un código que podía destruir la memoria del rival o impedir su correcto funcionamiento, y mostrar un mensaje en la pantalla. También diseñaron otro programa llamado Reeper, el equivalente a lo que es ahora un antivirus, cuya función era destruir cada copia hecha por Creeper. Conscientes de la peligrosidad del juego, se prometieron mantenerlo en secreto. En 1983 el Dr. **Thompson** dio a conocer estos programas, y la revista *Scientific American* publicó las guías para la creación de virus.



Una versión modificada del programa **CoreWar**, corriendo en un simulador **pMARS**.



Spam. Correo electrónico no solicitado. Mensajes de correo electrónico de tipo publicitario no solicitados, enviados en forma masiva a los usuarios registrados en diversos servidores de correo.

Desde 1974, *Xerox Corporation* presentó en Estados Unidos el primer programa que ya contenía un código auto duplicador. Los equipos Apple II se vieron afectados a fines de 1981 por un virus llamado **Cloner**, que presentaba un pequeño mensaje en forma de poema. Se introducía en los comandos de control e infectaba los discos cuando se hacía un acceso a la información utilizando el comando infectado.

En 1983, el **Dr. Fred Cohen** (1956-) presentó en la Universidad del Sur de California el primer *virus residente en una PC*, por lo que hoy se le conoce como el *Padre de los Virus Informáticos*. **Cohen** demostró que el código de programas para computadora podía auto replicarse, introducirse a otros códigos y alterar el funcionamiento de las computadoras.

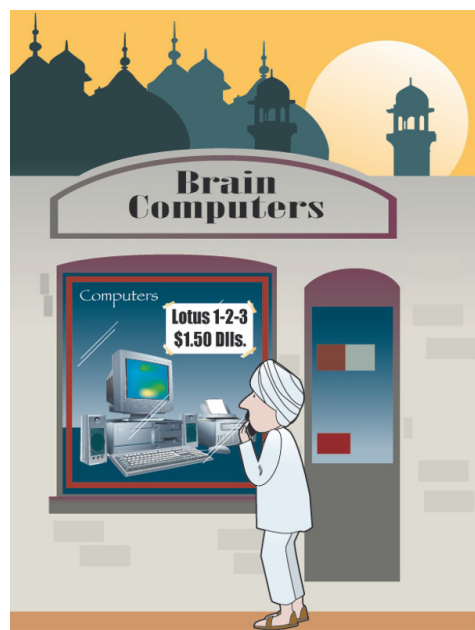
En 1986, es cuando ya se difunde ampliamente un *virus* con la finalidad de causar destrozos en la información de los usuarios. Este ataca una gran cantidad de computadoras en todo el mundo. Fue desarrollado en Lahore, Pakistán, por dos hermanos que comercializaban computadoras y *software*. Uno de ellos escribió un programa administrativo de gran utilidad, que vendían muy poco, porque todos lo copiaban y se lo distribuían entre sí.

Cansados de sufrir por la *piratería*, decidieron vender *copias ilegales* de programas populares como Lotus 1-2-3, y en éstos, así como en su propio programa, introdujeron un *virus benigno* con código muy elegante, el cual permitió que otros programadores lo modificaran para hacer de él, en sus nuevas versiones, uno de los virus más dañinos, conocido como virus **Brain** o **Paquistaní**, que se supone que infectó más de 30,000 computadoras solamente en Estados Unidos.



El Dr. **Fred Cohen**, inventor del primer virus de computadoras auto replicable.

Nota: Informaciones posteriores encontradas en *CompuServe*, red de servicios informativos de nivel internacional, anunciaban infecciones del virus **Brain**, que habían borrado archivos de estudiantes de la *Universidad de Miami*, de una editorial, y de un periódico. También se decía que, a causa de ese mismo virus, se habían destruido discos de algunos estudiantes de *Maryland*. Acerca de la versión difundida en México, nunca se supo que borrara archivos, pero sí inutilizaba los disquetes marcando sectores buenos como defectuosos.



Los hermanos **Basit** y **Amjad** vendían programas piratas con el virus de **Paquistán** o **Brain**, en su tienda *Brain Computer Services*.



Las computadoras Amiga Commodore, fueron atacadas en noviembre de 1987 por un virus que infectaba el sector de carga y se posicionaba en la memoria de la computadora. Al introducir otros disquetes quedaban infectados en la misma área de arranque, por lo que, al circular a través de otras computadoras, diseminaban el contagio.

En diciembre de 1987, los expertos de *IBM* tuvieron que diseñar un *programa antivirus* para desinfectar su sistema de correo interno, pues éste, fue contagiado por un virus no dañino que hacía aparecer en las pantallas de las computadoras conectadas a su red un mensaje navideño, el cual al reproducirse a sí mismo múltiples veces hizo muy lento el sistema de mensajes de la compañía, hasta el punto de paralizarlo por espacio de setenta y dos horas.

El virus presentaba un mensaje navideño con un árbol al lado, y pedía al usuario que tecleara la palabra **CHRISTMAS**. Si se tecleaba la palabra, el virus se introducía en la lista de correspondencia de correo electrónico del operador y se seguía diseminando por toda la red. Cuando no se accedía a la demanda y se apagaba el equipo, el virus impedía que se pudieran grabar los trabajos inconclusos, perdiéndose así muchas horas o días de trabajo.

En 1988 se identificó el *virus de Jerusalén* que, según algunas versiones, fue creado por la *Organización para la Liberación de Palestina* con motivo de la celebración del aniversario número cuarenta del último día en que Palestina existió como nación, el viernes 13 de mayo de 1988 (por eso el virus también se conoció como del **viernes 13**).

El uso de programas originales evita en un gran porcentaje la posibilidad de infección viral. Sin embargo, *Aldus Corporation*, una empresa de gran prestigio lanzó al mercado discos originales de su programa *FreeHand* para Macintosh, infectados por un **virus benigno** llamado **Macintosh Peace**, **MacMag** o **Brandow**. Este virus se desarrolló para poner un mensaje de paz en las pantallas de las computadoras, a fin de celebrar el aniversario de la introducción de la *Macintosh II*, el 2 de marzo de 1988.

La Nuclear Regulatory Commission, de Estados Unidos, anunció el 11 de agosto de 1988 su intención de sancionar hasta con \$1,250,000 dólares a la planta de energía nuclear *Peach Bottom*, en Pensilvania, porque sorprendió a los operadores de la planta jugando en las computadoras con copias piratas de programas de juegos.



Los operadores de la planta nuclear de *Peach Bottom* jugaban en la computadora con copias piratas de programas de juegos (ilustración del libro *Virus en las computadoras* de 1994, de Gonzalo Ferreyra Cortés).

El 2 de noviembre del mismo año 1988, las redes *ARPANET* y *NSFnet* en Estados Unidos, fueron infectadas por un *virus gusano* que se introdujo en ellas, afectando a más de 6,000 equipos de instalaciones militares de la *NASA*, universidades y centros de investigación públicos y privados.

También, el gusano invadió la naciente red *Internet*. Fue creado por **Robert Tappan Morris**. (1965-), estudiante de Harvard de 23 años, e hijo de uno de los creadores de **CoreWar**. Después de un juicio, fue condenado a tres años de libertad condicional, una multa de \$10,000 dólares y 400 horas de trabajo social.

En Estados Unidos, se formó una asociación de profesores, programadores y empresas de software, para estudiar, investigar y clasificar a los virus, con la finalidad de diseñar y elaborar medidas de protección y programas antivirus, de una manera coordinada, evitando así esfuerzos vanos en la titánica lucha que se echaban encima; la **CVIA**, **Computer Virus Industry Association**, con sede en Santa Clara, California.

En octubre de 1989 ya se visualizaba a los virus como una terrible epidemia, y empezaron a suceder hechos deplorables. Un comunicado de un desconocido comando tecno-terrorista manifestaba que había infectado una gran cantidad de computadoras, y que el viernes 13 se destruirían automáticamente los archivos almacenados en disquetes o en discos duros, desatando el pánico entre los usuarios, el cual estaba fundado básicamente en la superstición que provoca esa fecha.

Aunque no se realizó esta catastrófica profecía, sirvió para replantear el grave peligro al que están expuestos los datos de cualquier sistema. Esta tesis se refuerza con la publicación del 30 de octubre en el diario *The New York Times*, la cual anunciaba que las computadoras de la NASA habían sido interferidas por desconocidos causando problemas en el lanzamiento del transbordador espacial *Atlantis*.

En Estados Unidos, unas sesenta computadoras de la NASA fueron infectadas en esa ocasión y el programa intruso se siguió reproduciendo por medio de la red comercial que tenía la NASA con empresas privadas en aquel país. Se estima que muchos grandes bancos de datos internacionales y más de medio millón de PC fueron atacados por diversos tipos de virus.

En España también se propagaron varios tipos de virus, al grado de que una conocida revista de computación que incluía discos con programas en cada ejemplar distribuyó copias de esos discos contagiados con el virus de **Jerusalén** en uno de sus números de 1990. La revista reconoció públicamente su error y, además de retirar los ejemplares del mercado, en el siguiente número distribuyó discos de programas que contenían un antivirus para combatir al mencionado virus.

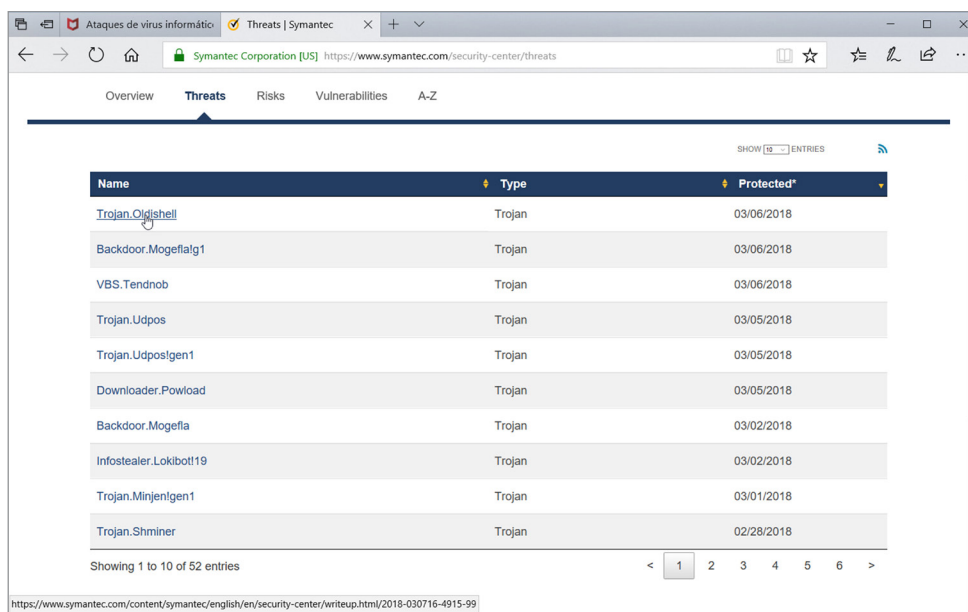
El colmo del terrorismo viral fue que, hasta los mismos programas vacunas, que se supone deberían ser los más confiables, fueron modificados por los ciberpunks –como se les ha llamado también a los programadores de los virus–. De esta manera el magnífico programa *FluShot*, que se difundió por medio de los **Bulletin Board Services** (BBS) de aquel entonces, infectó los sistemas de cientos de usuarios que veían en él, un programa de bajo costo y con muy buenas perspectivas en la lucha contra los virus.

En la actualidad, es difícil seguir el paso (con tanto detalle) a los virus informáticos, porque cada día aparecen decenas de nuevas cepas o variantes de ellas. Sin embargo, las empresas dedicadas a la seguridad informática, y a desarrollar programas antivirus, llevan listas detalladas y actualizadas de los reportes de virus que les llegan de todas partes del mundo.



Robert Tappan Morris, creador del primer gusano de Internet, que infectó a más de 6,000 computadoras en 1988.





Name	Type	Protected*
Trojan.Ojgishell	Trojan	03/06/2018
Backdoor.Mogefalg1	Trojan	03/06/2018
VBS.Tendnob	Trojan	03/06/2018
Trojan.Udpos	Trojan	03/05/2018
Trojan.Udpostgen1	Trojan	03/05/2018
Downloader.Powload	Trojan	03/05/2018
Backdoor.Mogefla	Trojan	03/02/2018
Infostealer.Lokibot!19	Trojan	03/02/2018
Trojan.Minjengen1	Trojan	03/01/2018
Trojan.Shminer	Trojan	02/28/2018

Showing 1 to 10 of 52 entries

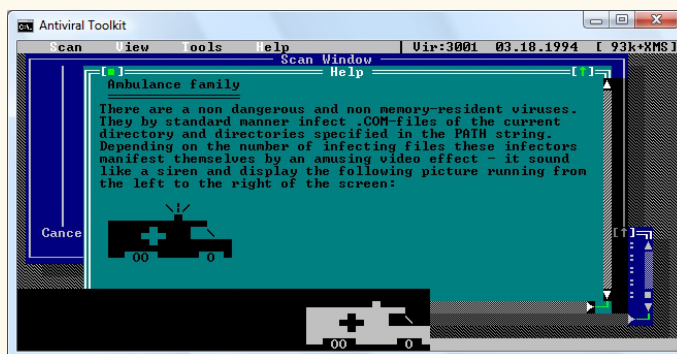
Las empresas creadoras de programas antivirus hacen un seguimiento diario de los reportes de virus que les llegan, o que detectan y ofrecen la solución en actualizaciones vía Internet.

Los principales virus informáticos

Al inicio de la computación personal, los virus que se descubrían tenían códigos y funcionamientos diferentes: objetos que se movían por la pantalla, pantallas que se volteaban de cabeza, cambio de los colores de las pantallas, sonidos extraños, etcétera. Esto se debía en gran parte a la facilidad de programación en el ambiente MS-DOS y Windows, y a su popularidad. Desde los primeros virus, los más conocidos han sido:

- **AIDS.** También conocido como *Hahaha*, *Taunt*, *SIDA* o *VGA2CGA*, es un virus infectador de archivos ejecutables. Al activarse presenta un mensaje en la pantalla: “*Your computer now has AIDS*”. El virus infecta los archivos ejecutables posicionándose en los primeros 13 kB, por lo que, al eliminarlo con cualquier antivirus, los programas quedan inservibles.
- **AirCop.** Virus residente en memoria descubierto en Estados Unidos en el año de 1990, de origen Taiwanés, que infectaba el sector de arranque de los disquetes. Era un virus muy dañino, ya que destruía los datos del sector 719, que es a donde enviaba el programa de carga original. Sólo infectaba disquetes de 360 kB, de 5 $\frac{1}{4}$ ”, y decrementaba la memoria de la computadora en 1024 bytes al instalarse. Bloqueaba y utilizaba las interrupciones 12h, 13h y 1Bh para controlar la computadora. Aleatoriamente, desplegaba el mensaje “*Red State, Germ Offensive. AIRCOP*”, y generalmente no infectaba ni el sector de carga, ni la tabla de particiones de los discos duros.
- **Ambulance Car.** Virus de archivos ejecutables que, al ejecutarse, de manera aleatoria se presentaba una imagen de una ambulancia que barría la parte inferior de la pantalla de izquierda a derecha, mientras se escuchaba el sonido característico de una sirena.

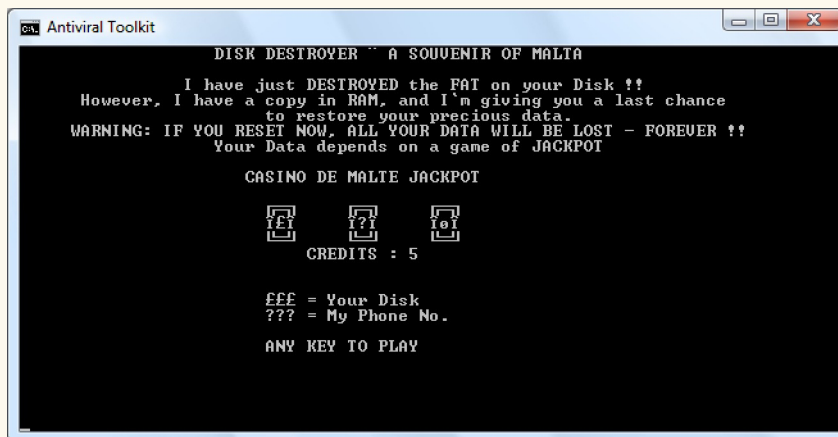
El antivirus ruso **AVP**, contenía simuladores de virus que permitían ver cómo funcionaban los más conocidos de entonces, como el **Ambulance**.



- **April 1st.** También conocido como *Surviv*, atacaba los archivos con extensión **.com** (ejecutables), excepto el **COMMAND.COM**. Presentaba en la pantalla un mensaje “*April 1st Ha Ha Ha You have a virus*”. Se activaba el primero de abril, tan pronto como se ejecutaba cualquier archivo **.com** infectado, se posicionaba en la memoria para esperar la ejecución de otro archivo, para infectarlo también. La siguiente versión, **April 1st B**, ya infectaba, programas ejecutables con extensión **.exe**.



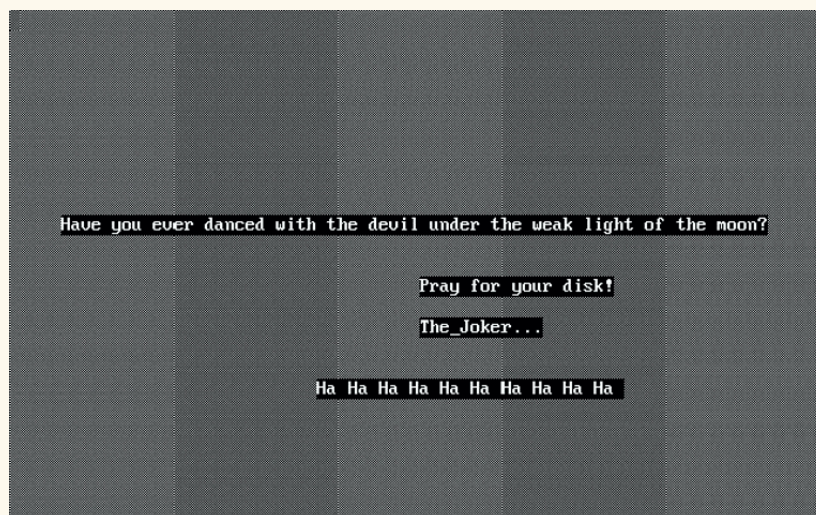
- **Boot Sector.** Es un virus originario de la ex Alemania Occidental que atacaba a las computadoras Atari modelo ST, alojándose en el sector de carga de los discos. Cuando se realizaba la carga inicial del sistema con el disco infectado, el virus se activa en la memoria de la computadora agregándose al vector de llamadas del sistema, que es el que controla todos los accesos al disco.
- **Brain o de Pakistán.** Infeccionador del sector de arranque, que sufrió una serie de mutaciones, adiciones y modificaciones. Conocido también como *Paquistaní, Nipper, Mente Paquistaní, Clone, Brain Ashar* y *Brain Singapore*, es el mismo que desarrollaron los hermanos que vendían productos de computación en Lahore, Pakistán. Marcaba tres *clusters* como dañados, hasta que no cabía nada más en el disco.
- **Casino.** Afortunadamente no fue un virus muy común, ya que el concepto destructivo azaroso, se prestaba para que algunos usuarios aventureros se jugaran la integridad de sus datos. El propósito de este virus era borrar la tabla de asignación de archivos del disco duro. Al activarse, hacía una copia de la FAT en la memoria RAM y borraba los datos del disco. Enseguida presentaba una pantalla con un juego de azar. Se contaba con cinco oportunidades para lograr que las tres maquinillas giratorias cayeran en **???** Si caían tres signos **£££**, el virus cumplía su cometido; se borraba la FAT y el disco quedaba sin tus datos.



Si tenías mucha suerte y le ganabas al virus, se desplegaba en la pantalla un mensaje ofensivo por ganarle.

- **Cascade** (*Virus de cascada*). Se le conoció también como *Falling Tears*, *Autumn Leaves*, *BlackJack*, *Fall*, *Falling Letters*, *1704* y *Cascade-1706*. Originado a finales de 1987, es producto de un Caballo de Troya modificado y producía la caída del texto a la parte inferior de la pantalla. Infectaba los archivos **.com**, aumentando su tamaño en 1,701 bytes.
- **Cookie** (*Virus de la galletita*). Se cuenta de un *virus gastronómico* que contagió las computadoras *DECsystem 10*. Este pequeño personaje permanecía latente por tiempo indefinido, y cuando se activaba presentaba en la pantalla el mensaje:
I WANT A COOKIE! (¡QUIERO UNA GALLETITA!).
Al teclear la palabra **COOKIE**, se lograba desactivarlo durante algún tiempo. La versión *Cookie 2232*, incluso al recibir la palabra **COOKIE**, desplegaba en la pantalla el mensaje *BURPS...*
- **Dark Avenger**. Virus originario de Bulgaria, conocido además como *Eddie*, *Diana*, *VAN Soft*, *Black Avenger*, *Rabid Avenger*, *Evil Men* y otros, fue descubierto en septiembre de 1989. Este virus infectaba los archivos ejecutables. Cada decimosexta infección enviaba parte de su código a escribir en sectores seleccionados aleatoriamente, destruyendo los datos ahí contenidos.
- **Devil's Dance** (*Baile del diablo*). Es un virus del tipo TSR (*Terminate and Stay Resident*) que fue desarrollado en México a fines de 1989. Infectaba archivos ejecutables **.com**, incluyendo al *COMMAND.COM*. Medía sólo 941 bytes. Infectaba al mismo programa varias veces, hasta crecerlo arriba de los 64 kB, lo que hacía que el sistema operativo MS-DOS ya no lo reconociera como archivo **.com** y no lo ejecutaba.

Cuando se activaba en la memoria de la computadora y se intentaba eliminarlo restableciendo el sistema pulsando las teclas **Ctrl + Alt + Supr**, presentaba en la pantalla el mensaje “¿Has bailado con el diablo bajo la tenue luz de la luna? ¡Reza por tu disco! El Guasón”. Si permanecía residente en la memoria de la computadora, después de teclear unos 5,000 caracteres, borraba la primera copia de la *FAT* del disco.



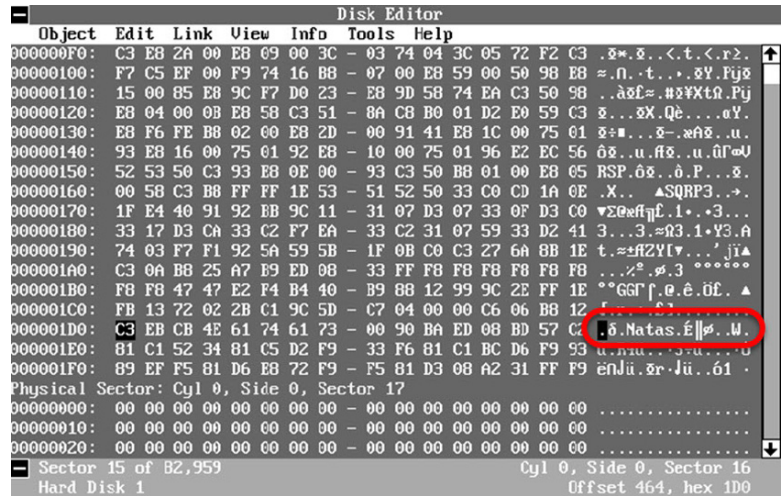
- **Eggbeater**. No se trata en realidad de un virus informático, sino de un Caballo de Troya que erróneamente, por sus características, se ha identificado como un virus. A diferencia de otros Caballos de Troya, *Eggbeater* cuando se ejecuta no manifiesta actividad alguna en la pantalla del monitor, pero a partir del momento en que se activa comienza a borrar todos los archivos que haya en los discos del sistema.
Una vez que ha concluido su destructiva labor, visualiza en la pantalla el mensaje *ARF, ARF! Gotcha!* La razón por la que no se considera como virus es que no tiene la capacidad de duplicar su código, lo cual es la principal característica de los virus informáticos.

- **Flip.** En la Alemania Oriental de 1990, se descubrió este virus suizo, cuya longitud es de 2,343 bytes. Se clasifica dentro de los infectores de archivos ejecutables con extensión **.com**, **.exe** y **overlays**, pero también corrompe los datos de la tabla de particiones y el sector de arranque de los discos duros. Encriptaba –codificaba– su código dentro de los programas infectados gracias a un algoritmo que no tiene más de 2 bytes, por lo que era de tipo polimorfo (*Polymorphic*). Los días 2 de cada mes, entre las 4 y 4:59 de la tarde, cuando estaba activo en la memoria de la computadora y ésta contaba con un monitor VGA o EGA, el virus *Flip* “volteaba” la pantalla; es decir ubica lo de arriba abajo y viceversa –de ahí su nombre *Flip*–.
- **Friday the 13th.** También llamado *Virus Com* o *Virus 512*. Aunque lleva el mismo nombre, no es el mismo que el conocido *viernes 13* de *Jerusalén*. Se mantenía activo en la memoria e infectaba los archivos **.com**. Su origen se situó en Sudáfrica en 1987. Cuando se ejecutaba buscaba dos archivos **.com** en el disco duro y uno en la unidad A, y los infectaba. Era muy veloz y casi no se detectaba su acceso al disco; si se ejecutaba los viernes 13, borraba el programa anfitrión –igual que el virus de *Jerusalén*–.
- **Italian.** Conocido también como de *Turín*, *Ping Pong* o de la *Pelotita*, es un segmento de código que, a diferencia de la mayoría de los virus, no modificaba los archivos ejecutables ni producía ningún daño a los discos, excepto infectarlos. Este virus grababa parte de su código en el área de carga inicial (*Boot area*) y, para no afectarla, traslada el programa de carga inicial al primer sector libre que encuentra y lo marca como defectuoso para que no sea sobrescrito. Algunos usuarios que padecieron este desagradable virus en sus sistemas, se acostumbraron a vivir con él, y cuando aparecía la *pelotita*, la única solución que aplicaban era, apagar la computadora y esperar que en la próxima sesión de trabajo no se presentara.
- **Michelangelo.** El virus *Michelangelo* se activaba cualquier 6 de marzo, pues se cree que fue hecho para “celebrar” ese día el nacimiento de **Miguel Angel Buonarroti** (1475-1564), escultor, arquitecto y pintor italiano del Renacimiento. En esa fecha, si tu computadora estaba infectada con el virus, al “arrancar” el sistema con el disquete o disco duro “infectado”, lo primero que hacía éste es verificar la fecha del reloj del sistema. Si ésta coincidía, en lugar de infectar disquetes o el disco duro, sobrescribía el disco desde el cual se realizó la carga, destruyendo la información contenida en él.



Las computadoras tipo XT (de las primeras PC) se salvaban de la terrible acción del virus de **Miguel Angel** al encenderlas, porque cuando se cargaba el virus, todavía no estaba asignada la fecha en la memoria.

- **NATAS.** (*Satan al revés*). Este virus, posiblemente originario de San Diego, California, no se puede clasificar entre los infectores de sectores de carga, pero tampoco podría estar con los infectores de archivos ejecutables. La razón es que era un virus *Multipartita* (*Multipartite*), porque infectaba diferentes partes de los discos, como archivos ejecutables, controladores de dispositivos (**.sys**), sector de arranque y tabla de particiones, *Polimorfo* (*Polymorphic*), que significa que empleaba algoritmos de encriptación –codificación– para hacer más compleja su detección, y *Mutante* (aunque no en el estricto sentido de la palabra), características que lo convirtieron en un virus muy especial. El virus NATAS –así en mayúsculas– realmente marcó el principio de una época, por lo menos en México, porque se consideró que en el año de 1994 tan sólo entre los meses de febrero a agosto, había infectado por lo menos a una computadora del 95% de las empresas públicas y privadas; en la figura se muestra el sector 15 de un disco infectado por el virus *Natas*. Todos los días se sabía de infecciones a causa de este virus en bancos, oficinas de gobierno, institutos de investigaciones, escuelas de todos los niveles y usuarios personales.



A.3 Virus informáticos en la actualidad

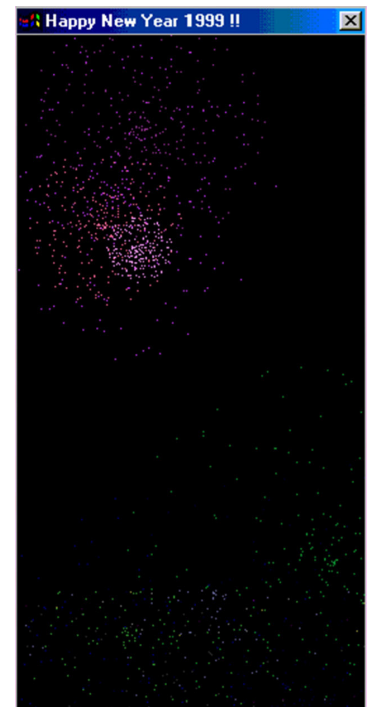
Tal vez uno de los virus que cierra la historia antigua de los virus de computadoras, fue **I.Worm.Happy**, también conocido como *Happy99*, *Happy*, *Trojan.Happy99*, *W32/Ska-Happy99*, *Ska*, *Ska.exe*, *W32/Ska.A* y otros alias, descubierto en enero de 1999. Era un gusano que afectaba las computadoras con sistema operativo Windows 95 y Windows 98. Dejó esa marca, porque a diferencia de los virus antiguos que se diseminaban a través de disquetes o en programas piratas, se distribuyó mediante la red Internet, como documento adjunto de correo electrónico, que es la vía de infecciones en la actualidad.

Cuando “explotaba” la bomba, aparecía una ventana emergente (*Pop-up*) de Windows, con el mensaje **Happy New Year!!**

■ Principales virus actuales

Es a partir de la proliferación de las redes, de Internet y específicamente, de la *World Wide Web*, que los virus cambiaron su forma de distribución y algunas veces sus cometidos; ahora no se trata sólo de borrar las áreas críticas de los medios de almacenamiento, sino de “molestar” y rastrear datos importantes para robar identidades, contraseñas y, por supuesto, cuentas bancarias.

- **I loveYou.** Conocido también como *Love Bug* o *Love Letter*, es un gusano que se reproduce a través de las redes, modifica los archivos de la computadora afectada y se transmite a través del correo electrónico, cuando se abre el archivo adjunto donde se aloja.



Comenzamos con este virus por dos razones; el inicio de una nueva era de programas denominados *malware*, y su importancia; en mayo del año 2000 se esparció este virus de origen filipino, como un archivo adjunto al correo electrónico con el nombre “LOVE-LETTER-FOR-YOU.TXT.vbs”, infectando a más de 50 millones de computadoras, con pérdidas de miles de millones de dólares.

- **AutoRun.MXS.** Troyano de bajo peligro, que llega al sistema como archivo adjunto de correo enviado de forma masiva. Vigila las actividades del usuario en el navegador Internet Explorer e intenta descargar otros códigos maliciosos. Es posible eliminarlo con la función de restauración del sistema de Windows Me, Windows XP y Windows Vista.
- **Code Red (Código Rojo).** Se trata de un gusano que se auto copia de máquina en máquina a través de las redes. Se considera que este virus ha sido uno de los más destructivos de los últimos tiempos, ya que reprodujo más de 250,000 copias de sí mismo en un solo día.
- **Email-Worm.Win32.Warezov.nf.** El 19 de enero de 2009 apareció en Internet la nueva modificación del gusano Warezov, que se considera de riesgo moderado a alto. La forma de infectar es parecida al *Email-Worm.Win32.Warezov.mx*.
- **I-Worm.Sircam.c.** Este gusano de Internet cuyo origen se atribuye a México se ha escrito en Delphi y tiene cerca de 130K. Se distribuye mediante el correo electrónico y se reproduce a una gran velocidad, de tal manera, que en un solo día infectó a miles de usuarios de Internet, quienes vivieron una pesadilla al perder sus archivos y programas.
- **Net-Worm.Win32.Kido.** Descubierta en enero de 2009, es un virus de riesgo moderado que tiene múltiples variantes de *Kido*. Es un virus polimórfico que se está propagando ampliamente mediante redes locales y medios de almacenamiento extraíbles. Desactiva el modo de restauración del sistema operativo, bloquea accesos a sitios web de seguridad informática, y descarga malware adicional en los equipos infectados.
- **Nimda.L.** Virus infectador de archivos ejecutables de origen chino, que se distribuye en la red Internet al acceder a páginas web infectadas, o a redes con recursos compartidos. Esta variante se detectó el 16 de junio de 2003, y se activa al ejecutarse los archivos *_setup.exe* y *riched20.dll*, que infectan a todos los archivos ejecutables a su paso.
- **SpyEye.** Aplicación *malware* diseñada en el año 2011, para dispositivos Apple, que ataca a los usuarios de los navegadores *Safari*, *Google Chrome*, *Firefox*, *Internet Explorer* y *Opera*, ya sea en sistemas operativos IOS de Apple o Microsoft Windows. Este *malware* del tipo *secuestrador* detecta y registra las pulsaciones de las teclas y el llenado de formularios para robar los datos de las cuentas bancarias e iniciar transacciones fraudulentas, aun cuando el usuario original esté en una sesión en su cuenta bancaria.
- **VBS.Rowam.A.** Pequeñísimo troyano de sólo 2,749 bytes, que cuando infecta trata de borrar archivos alojados en el disco duro. Puede enviar mensajes de correo electrónico a todos los recipientes de la libreta de direcciones, aunque esta no es su manera de propagación. Los mensajes enviados muestran el mensaje “Free MSN Upgrade” en el campo **Asunto**.
- **W32/Bugbear.B.** Esta variante del destructivo gusano *Bugbear* se distribuye en Internet, en los mensajes de correo electrónico. Los archivos anexos que contiene se muestran con dos extensiones que pueden ser **.scr**, **.pif**, o **.exe**. Deshabilita los antivirus y burla a los *firewalls* para infectar archivos de sistema. Facilita a los *hackers* tomar el control de un sitio, desde un lugar remoto.
- **WannaCry ransomware attack.** Apenas en mayo de 2017 se descubrió una aplicación (conocida como *criptogusano*) de *malware*, de la familia *WannaCry*, cuya finalidad es atacar al sistema operativo Windows, encriptando los datos del usuario de la computadora; para liberar los datos, pide un rescate, que se debe pagar con la ciber moneda *Bitcoin*, para permitir el acceso a los datos, desencriptándolos.

- **Win32/Lafee.B.** Se le conoce también con los nombres *Win32/Lafee.B*, *Virus.Win32.Daum.a*, *Virus.Win32.Daum.a* y *Mal/Generic-A*. Es un virus infectador de archivos ejecutables con extensiones **.exe** y **.scr**, y descarga de Internet otros tipos de *malware*.
- **W32.Mydoom.AI@mm.** Descubierto el 16 de enero de 2005, este gusano que se distribuye de manera masiva por correo electrónico, utiliza su propio protocolo SMTP para enviarse a todos los contactos almacenados en la computadora. Al infectar crea los archivos *Isasrv.exe*, *version.ini* y *hserv.sys*, donde almacena una copia de sí mismo, un texto y un archivo binario. Intenta desactivar los procesos de seguridad que se ejecutan en computadoras con elementos de seguridad como firewalls y antivirus.
- **Zhelatin.o.** En febrero de 2009 se detectó envío masivo de este virus por Internet, como archivo adjunto de mensajes de correo infectados. En el campo **Asunto** presenta mensajes como: *I Always Knew; I Believe; I Love You Soo Much; I Love You with All I Am; I Still Love You*, etcétera.

A.4 Seguridad de la información

La manera más común de adquirir un virus informático siempre fue a través de copias ilegales de programas. Por esta razón, por sentido común y por norma ética, como primer consejo: no debes copiar los programas originales para distribuirlos ilegalmente entre tus amigos; ¡y mucho menos para venderlos!

Programas antivirus

A partir de la proliferación de los virus informáticos, se ha desarrollado también una industria dedicada a la creación de programas llamados *vacunas* o *antivirus*, que tienen como finalidad detectarlos, erradicarlos y prevenir las infecciones virales.

Los programas antivirus actuales han tenido que evolucionar, ahora ofrecen esquemas completos de seguridad que incluyen desde aplicaciones para crear copias de seguridad, hasta programas que realizan análisis de virus y software espía, protección integral tipo *firewall*, revisión de mensajes de correo electrónico y por supuesto, la función de actualización de las vacunas, que es de lo más importante.

Las siguientes direcciones de Internet son de compañías confiables, dedicadas al desarrollo de antivirus. Algunas de las empresas ofrecen versiones de evaluación o gratuitas. También las hay que permiten revisar en línea el disco duro de tu computadora, de manera gratuita, para desinfectar el disco si contiene algún virus conocido, o amenazas de *malware*:

<https://www.bitdefender.es/>

<https://www.mcafee.com/mx/index.html>

<https://mx.norton.com/>

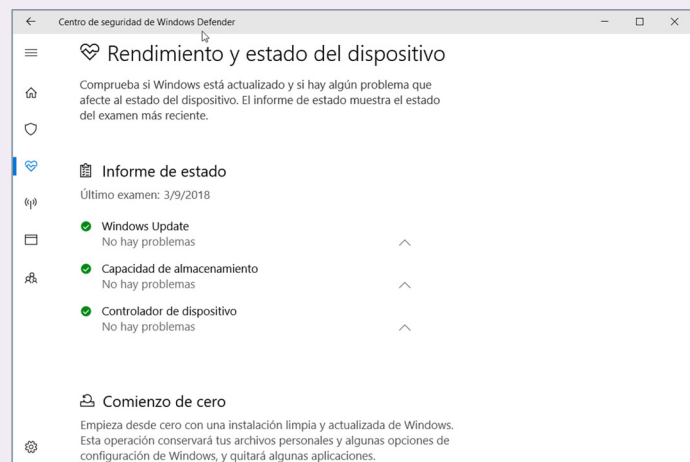
<https://www.pandasecurity.com/mexico/>

<https://www.scanguard.com/>

<https://www.totalav.com/>

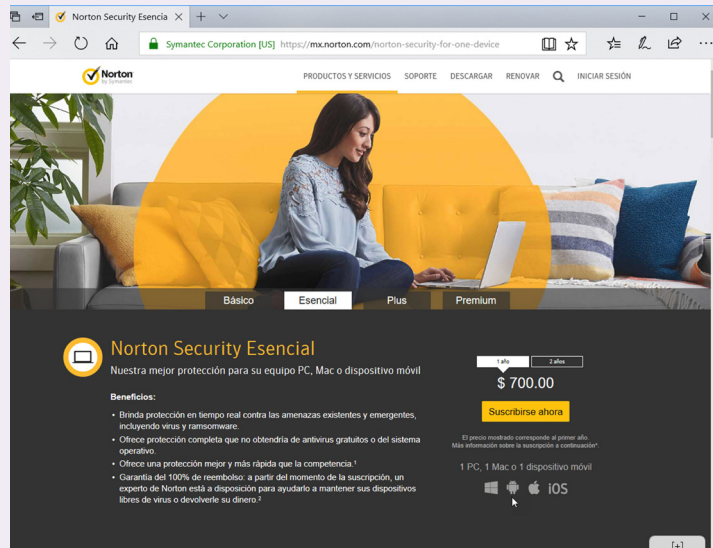
<https://latam.kaspersky.com/>

- **Windows Defender.** Desde la aparición de Windows Vista, Microsoft liberó un programa de seguridad, antivirus, llamado *Live One Care*, para competir con las compañías más reconocidas en cuanto a programas antivirus. Windows 10 ofrece un servicio de seguridad llamado *Windows Defender*, que permite proteger tu computadora contra virus, *malware*, *spyware* y otras amenazas.

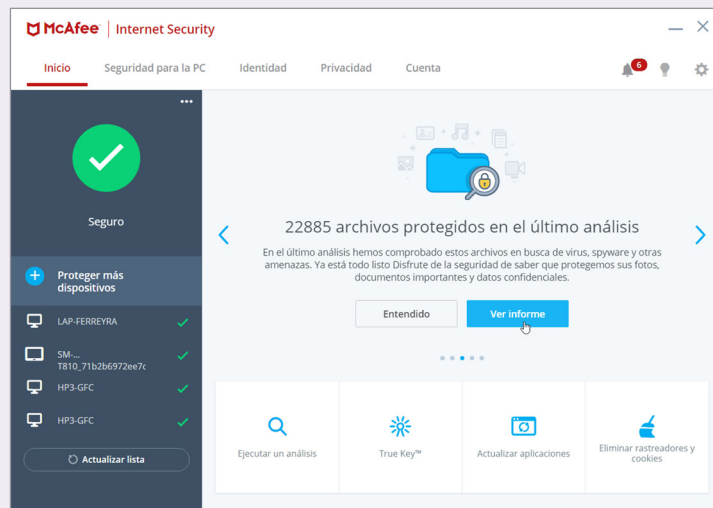


Microsoft ofrece un servicio completo de seguridad, gratuito, para los usuarios del sistema operativo Windows 10.

- **Norton Antivirus.** Desde siempre, *Peter Norton computing*, hoy *Symantec Corporation*, se destacó por sus programas de utilerías, como *Norton Utilities*, *Norton Disk Doctor*, *Speed Disk*, *Norton SymantecWorks*, y otros, ya que el **Dr. Peter Norton** (1943-) se especializó en el trabajo interno de las computadoras, especialmente en el disco duro, con su *Norton Utilities*, que también ha sido una de las mejores aplicaciones de utilidades, edición y reparación lógica de discos duros. Actualmente, los programas de seguridad de Symantec están considerados entre los mejores programas de protección de computadoras.
- **McAfee.** Otro de los antivirus más antiguos y confiables es *McAfee*, que en algún tiempo estuvo bajo la dirección de **John McAfee** (1945-), recuerda que fue director de la *Computer Virus Industry Association*, una asociación de empresas dedicadas a luchar contra los *hackers* y los *crackers* creadores de virus. Las aplicaciones de McAfee son muy utilizadas en los hogares, en las pequeñas y grandes empresas, y ahora, hasta por los usuarios de dispositivos móviles, que también están expuestos a los virus que se distribuyen mediante las redes e Internet.



Symantec cuenta con aplicaciones de seguridad contra virus, amenazas y espías, de indudable calidad, además de protección de redes.



Con *McAfee Internet Security* puedes estar seguro al recibir tus mensajes de correo electrónico y visitar páginas web.



- **Kaspersky Lab.** Otro pionero de la lucha contra los virus informáticos es **Eugene Kaspersky** (1965-), programador ruso, que se interesó por los virus informáticos desde muy joven (Figura 1.64). En la actualidad es el dueño de su propia empresa; **Kaspersky Antivirus**, con más de 900 empleados en varios países. Kaspersky Lab siempre ha tenido diversos servicios de información para los usuarios, como la Enciclopedia de virus, donde se proporciona abundante información de la mayoría de los virus conocidos, y medidas de protección.

Los antivirus sólo son eficientes cuando se *actualizan periódicamente*, ya que en cada actualización se incluyen los códigos de los nuevos virus descubiertos. Las empresas dedicadas a combatir a los virus de computadoras actualizan la base de datos por lo menos cada semana, y en casos de urgencia, sacan una actualización el mismo día en que se detecta una nueva variante de un virus peligroso.



■ 10 medidas básicas de seguridad

Se ha visto que la única solución viable contra los virus, ya que son programas, es estudiar las cadenas de caracteres que componen su código, y compararlas con una base de datos que incluye una muestra de cada uno de los virus identificados previamente. Cuando coinciden los códigos, el antivirus está seguro de haber encontrado un virus, y procede contra él. Por esto, lo más importante es actualizar los antivirus, para estar siempre protegidos de los nuevos virus

1. **No** utilices copias ilegales o piratas de los programas.
2. **No** olvides crear respaldos o copias de seguridad de toda la información generada, diaria y semanalmente.
3. **No** olvides discos o unidades de almacenamiento en las unidades lectoras. Si el medio de almacenamiento está infectado, fácilmente se puede contagiar la computadora.
4. **Protege** contra escritura los medios de almacenamiento que tengas que introducir a una computadora extraña.
5. **No** permitas que personas desconocidas introduzcan unidades USB o discos compactos de dudosa procedencia en tu computadora.
6. **Protege** los accesos a la red con contraseñas (*passwords*).
7. **Configura** correctamente las opciones de **Correo electrónico no deseado** de Outlook.
8. **No** abras todos los correos electrónicos que te llegan, sobre todo cuando desconozcas quién te los envía, o su procedencia.
9. **No** “descargues” archivos de sitios web desconocidos, sobre todo, no los ejecutes en tu computadora si no los revisas antes con un antivirus actualizado.
10. **¡Instala un programa antivirus, y mantenlo siempre actualizado!**

A.5 Reafirmación del aprendizaje

1. Dividan la clase en grupos de cuatro alumnos y realicen las siguientes tareas e investigaciones:
 - a) Que cada uno de los grupos investigue en buscadores de Internet acerca de los siguientes temas, y escriba en un documento de Word notas breves:
 - ¿Qué son los virus de computadoras?
 - ¿Cómo funcionan los virus de computadoras?
 - Principales características de los virus informáticos.
 - Métodos de propagación de los virus informáticos.
 - Clasificación de los virus de computadoras.
 - b) Inicien una sesión grupal donde se discutan los temas, exponiendo cada grupo las anotaciones de sus investigaciones.
 - Lleguen a conclusiones sobre cada uno de los temas propuestos.
 - ¿Quién creen que desarrolla los virus informáticos y con qué finalidad?
 - ¿Se necesita ser muy buen programador para crear virus informáticos?
 - c) Después de su sesión grupal, respondan las siguientes preguntas:
 - Escriban una definición breve que resuma lo que son los virus de computadoras.

- Describan brevemente tres de las principales características de los virus informáticos.

1. _____
2. _____
3. _____

- Escriban un breve resumen sobre la manera en que funcionan los virus informáticos.

- ¿A quién se conoce como el padre de los virus informáticos?
