VIRUS−MONOGRAFÍAS

- **¿CÓMO NACIERON LOS VIRUS?.**

Hacia finales de los años 60, Douglas McIlory, Victor Vysottsky y Robert Morris idearon un juego al que llamaron ***Core War*** (Guerra en lo Central, aludiendo a la memoria de la computadora), que se convirtió en el pasatiempo de algunos de los programadores de los laboratorios Bell de AT&T.

El juego consistía en que dos jugadores escribieran cada uno un programa llamado *organismo*, cuyo hábitat fuera la memoria de la computadora. A partir de una señal, cada programa intentaba forzar al otro a efectuar una instrucción inválida, ganando el primero que lo consiguiera.

Al término del juego, se borraba de la memoria todo rastro de la batalla, ya que estas actividades eran severamente sancionadas por los jefes por ser un gran riesgo dejar un *organismo* suelto que pudiera acabar con las aplicaciones del día siguiente. De esta manera surgieron los programas **destinados a dañar** en la escena de la computación.

Uno de los primeros registros que se tienen de una infección data del año 1987, cuando en la Universidad estadounidense de Delaware notaron que tenían un virus porque comenzaron a ver "© Brain" como etiqueta de los disquetes.

La causa de ello era Brain Computer Services, una casa de computación paquistaní que, desde 1986, vendía copias ilegales de software comercial infectadas para, según los responsables de la firma, dar una lección a los piratas.

Ellos habían notado que el sector de booteo de un disquete contenía código ejecutable, y que dicho código se ejecutaba cada vez que la máquina se inicializaba desde un disquete.

Lograron reemplazar ese código por su propio programa, residente, y que este instalara una réplica de sí mismo en cada disquete que fuera utilizado de ahí en más.

También en 1986, un programador llamado Ralf Burger se dio cuenta de que un archivo podía ser creado para copiarse a sí mismo, adosando una copia de él a otros archivos. Escribió una demostración de este efecto a la que llamó VIRDEM, que podía infectar cualquier archivo con extensión **.COM**.

Esto atrajo tanto interés que se le pidió que escribiera un libro, pero, puesto que él desconocía lo que estaba ocurriendo en Paquistán, no mencionó a los virus de sector de arranque (boot sector). Para ese entonces, ya se había empezado a diseminar el virus Vienna.

Actualmente, los virus son producidos en cantidades extraordinarias por muchisima gente alrededor del planeta. Algunos de ellos dicen hacerlo por divertimento, otros quizás para probar sus habilidades. De cualquier manera, hasta se ha llegado a notar un cierto grado de competitividad entre los autores de estos programas.

Con relación a la motivación de los autores de virus para llevar a cabo su obra, existe en Internet un documento escrito por un escritor freelance Markus Salo, en el cual, entre otros, se exponen los siguientes conceptos:

- Algunos de los programadores de virus, especialmente los mejores, sostienen que su interés por el tema es puramente científico, que desean averiguar todo lo que se pueda sobre virus y sus usos.

- A diferencia de las compañías de software, que son organizaciones relativamente aisladas unas de otras (todas tienen secretos que no querrían que sus competidores averiguaran) y cuentan entre sus filas con mayoría de estudiantes graduados, las agrupaciones de programadores de virus están abiertas a cualquiera que se interese en ellas, ofrecen consejos, camaradería y pocas limitaciones. Además, son libres de seguir cualquier objetivo que les parezca, sin temer por la pérdida de respaldo económico.
- El hecho de escribir programas vírales da al programador cierta fuerza coercitiva, lo pone fuera de las reglas convencionales de comportamiento. Este factor es uno de los más importantes, pues el sentimiento de pertenencia es algo necesario para todo ser humano, y es probado que dicho sentimiento pareciera verse reforzado en situaciones marginales.
- Por otro lado, ciertos programadores parecen intentar legalizar sus actos poniendo sus creaciones al alcance de mucha gente, (vía Internet, BBS especializadas, etc.) haciendo la salvedad de que el material es peligroso, por lo cual el usuario debería tomar las precauciones del caso.
- Existen programadores, de los cuales, generalmente, provienen los virus más destructivos, que alegan que sus programas son creados para hacer notoria la falta de protección de que sufren la mayoría de los usuarios de computadoras.
- La gran mayoría de estos individuos son del mismo tipo de gente que es reclutada por los grupos terroristas: hombres, adolescentes, inteligentes.

En definitiva, sea cual fuere el motivo por el cual se siguen produciendo virus, se debe destacar que su existencia no ha sido sólo perjuicios: gracias a ellos, mucha gente a tomado conciencia de qué es lo que tiene y cómo protegerlo.

- **¿QUÉ ES UN VIRUS?.**

Es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este. Decimos que es un programa parásito porque el programa ataca a los archivos o sector es de "booteo" y se replica a sí mismo para continuar su esparcimiento.

Algunos se limitan solamente a replicarse, mientras que otros pueden producir serios daños que pueden afectar a los sistemas. Se ha llegado a un punto tal, que un nuevo virus llamado W95/CIH−10xx. o también como CIH.Spacefiller (puede aparecer el 26 de cada mes, especialmente 26 de Junio y 26 de Abril) ataca al BIOS de la PC huésped y cambiar su configuración de tal forma que se requiere cambiarlo. Nunca se puede asumir que un virus es inofensivo y dejarlo "flotando" en el sistema.

Existen ciertas analogías entre los virus biológicos y los informáticos: mientras los primeros son agentes externos que invaden células para alterar su información genética y reproducirse, los segundos son programas−rutinas, en un sentido más estricto, capaces de infectar archivos de computadoras, reproduciéndose una y otra vez cuando se accede a dichos archivos, dañando la información existente en la memoria o alguno de los dispositivos de almacenamiento del ordenador.

Tienen diferentes finalidades: Algunos sólo 'infectan', otros alteran datos, otros los eliminan, algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: **PROPAGARSE**.

Es importante destacar que ***el potencial de daño de un virus informático no depende de su complejidad sino del entorno donde actúa***.

La definición más simple y completa que hay de los virus corresponde al modelo D. A. S., y se fundamenta en tres características, que se refuerzan y dependen mutuamente. Según ella, un virus es un programa que cumple las siguientes pautas:

- Es dañino
- Es autorreproductor

- Es subrepticio

El hecho de que la definición imponga que los virus son programas no admite ningún tipo de observación; está extremadamente claro que son programas, realizados por personas. Además de ser programas tienen el fin ineludible de causar daño en cualquiera de sus formas.

Asimismo, se pueden distinguir tres módulos principales de un virus informático:

- Módulo de Reproducción
- Módulo de Ataque
- Módulo de Defensa

El **módulo de reproducción** se encarga de manejar las rutinas de "parasitación" de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse subrepticiamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.

El **módulo de ataque** es optativo. En caso de estar presente es el encargado de manejar las rutinas de daño adicional del virus. Por ejemplo, el conocido virus **Michelangelo**, además de producir los daños que se detallarán más adelante, tiene un módulo de ataque que se activa cuando el reloj de la computadora indica 6 de Marzo. En estas condiciones la rutina actúa sobre la información del disco rígido volviéndola inutilizable.

El **módulo de defensa** tiene, obviamente, la misión de proteger al virus y, como el de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la remoción del virus y retardar, en todo lo posible, su detección.

- **TIPOS DE VIRUS.**

Los virus se clasifican por el modo en que actúan infectando la computadora:

- Programa: Infectan archivos ejecutables tales como .com / .exe / .ovl / .drv / .sys / .bin
- Boot: Infectan los sectores Boot Record, Master Boot, FAT y la Tabla de Partición.
- Múltiples: Infectan programas y sectores de "booteo".
- Bios: Atacan al Bios para desde allí reescribir los discos duros.
- Hoax: Se distribuyen por e−mail y la única forma de eliminarlos es el uso del sentido común.

Al respecto, se trata de virus que no existe y que se utiliza para aterrar a los novatos especialmente en la Internet a pesar que los rumores lo muestran como algo muy serio y a veces la información es tomada por la prensa especializada.

Por lo general, como ya se expresó, la difusión se hace por cadenas de e−mail con terribles e inopinadas advertencias. En realidad el único virus es el mensaje. A continuación se dan una serie de supuestos "virus", por lo que es aconsejable ignorar los mensajes que aparecen y no ayudar a replicarlos continuando con la cadena:

- 3b Trojan (alias PKZIP Virus).
- AOL4Free Virus Hoax.
- Baby New Year Virus Hoax.
- BUDDYLST.ZIP
- BUDSAVER.EXE
- Budweiser Hoax
- Death69

- Deeyenda
- E−Flu
- FatCat Virus Hoax
- Free Money
- Get More Money Hoax
- Ghost
- Good Times
- Hacky Birthday Virus Hoax
- Hairy Palms Virus Hoax
- Irina
- Join the Crew
- Londhouse Virus Hoax
- Microsoft Virus Hoax
- Millenium Time Bomb
- Penpal Greetings
- Red Alert
- Returned or Unable to Deliver
- Teletubbies
- Time Bomb
- Very Cool
- Win a Holiday
- World Domination Hoax
- Yellow Teletubbies
- A.I.D.S. hoax email virus
- AltaVista virus scare
- AOL riot hoax email
- ASP virus hoax
- Back Orifice Trojan horse
- Bill Gates hoax
- Bloat, see MPEG virus hoax
- Budweiser frogs screen−saver scare
- Good Times hoax email virus
- Irina hoax virus
- Java virus scare
- Join the Crew hoax email virus
- 'Millennium' virus misunderstanding
- MPEG virus hoax
- 'My clock says 2097/2098' virus misunderstanding
- New virus debug device hoax email virus with attached Trojan horse
- Open: Very Cool, see A.I.D.S. hoax email virus
- Penpal Greetings, see Good Times hoax email virus
- PKZ300 Trojan virus scare
- Returned or Unable to Deliver hoax email virus
- Walt Disney greeting, see Bill Gates hoax
- Win a Holiday hoax email virus
- Windows '98 MS Warning.

Por último, cabe destacar que los HOAX están diseñados únicamente para asustar a los novatos (y a los que no lo son tanto). Otros como el mensaje del carcinoma cerebral de **Jessica, Jessica Mydek**, **Anabelle**, **Ana**, **Billy** y otros personajes imaginarios tampoco son reales como tampoco lo es la dirección **ACS@aol.com**, ya que fueron creados para producir congestionamiento en la Internet.

- **CARACTERÍSTICAS DE LOS VIRUS.**

El virus es un pequeño software (cuanto más pequeño más fácil de esparcir y más difícil de detectar), que permanece inactivo hasta que un hecho externo hace que el programa sea ejecutado o el sector de "booteo" sea leído. De esa forma el programa del virus es activado y se carga en la memoria de la computadora, desde donde puede esperar un evento que dispare su sistema de destrucción o se replique a sí mismo.

Los más comunes son los residentes en la memoria que pueden replicarse fácilmente en los programas del sector de "booteo", menos comunes son los no−residentes que no permanecen en la memoria después que el programa−huesped es cerrado.

Los virus pueden llegar a "camuflarse" y esconderse para evitar la detección y reparación. Como lo hacen:

- El virus re−orienta la lectura del disco para evitar ser detectado;
- Los datos sobre el tamaño del directorio infectado son modificados en la FAT, para evitar que se descubran bytes extra que aporta el virus;
- encriptamiento: el virus se encripta en símbolos sin sentido para no ser detectado, pero para destruir o replicarse **DEBE** desencriptarse siendo entonces detectable;
- polimorfismo: mutan cambiando segmentos del código para parecer distintos en cada "nueva generación", lo que los hace muy difíciles de detectar y destruir;
- Gatillables: se relaciona con un evento que puede ser el cambio de fecha, una determinada combinación de tecleo; un macro o la apertura de un programa asociado al virus (Troyanos).

Los virus se transportan a través de programas tomados de BBS (Bulletin Boards) o copias de software no original, infectadas a propósito o accidentalmente. También cualquier archivo que contenga "ejecutables" o "macros" puede ser portador de un virus: downloads de programas de lugares inseguros; e−mail con "attachments", archivos de MS−Word y MS−Excel con macros. Inclusive ya existen virus que se distribuyen con MS−Power Point. Los archivos de datos, texto o Html **NO PUEDEN** contener virus, aunque pueden ser dañados por estos.

Los virus de sectores de "booteo" se instalan en esos sectores y desde allí van saltando a los sectores equivalentes de cada uno de los drivers de la PC. Pueden dañar el sector o sobreescribirlo. Lamentablemente obligan al formateo del disco del drive infectado. Incluyendo discos de 3.5" y todos los tipos de Zip de Iomega, Sony y 3M. (No crean vamos a caer en el chiste fácil de decir que el más extendido de los virus de este tipo se llama MS

Windows 98).

En cambio los virus de programa, se manifiestan cuando la aplicación infectada es ejecutada, el virus se activa y se carga en la memoria, infectando a cualquier programa que se ejecute a continuación. Puede solaparse infecciones de diversos virus que pueden ser destructivos o permanecer inactivos por largos periodos de tiempo.

- **DAÑOS DE LOS VIRUS.**

Definiremos **daño** como acción una indeseada, y los clasificaremos según la cantidad de tiempo necesaria para reparar dichos daños. Existen seis categorías de daños hechos por los virus, de acuerdo a la gravedad.

- **DAÑOS TRIVIALES.**

Sirva como ejemplo la forma de trabajo del virus **FORM** (el más común): En el día 18 de cada mes cualquier tecla que presionemos hace sonar el beep. Deshacerse del virus implica, generalmente, segundos o minutos.

- **DAÑOS MENORES.**

Un buen ejemplo de este tipo de daño es el **JERUSALEM**. Este virus borra, los viernes 13, todos los programas que uno trate de usar después de que el virus haya infectado la memoria residente. En el peor de los casos, tendremos que reinstalar los programas perdidos. Esto nos llevará alrededor de 30 minutos.

- **DAÑOS MODERADOS.**

Cuando un virus formatea el disco rígido, mezcla los componentes de la **FAT** (File Allocation Table, Tabla de Ubicación de Archivos), o sobreescribe el disco rígido. En este caso, sabremos inmediatamente qué es lo que está sucediendo, y podremos reinstalar el sistema operativo y utilizar el último backup. Esto quizás nos lleve una hora.

- **DAÑOS MAYORES.**

Algunos virus, dada su lenta velocidad de infección y su alta capacidad de pasar desapercibidos, pueden lograr que ni aún restaurando un backup volvamos al último estado de los datos. Un ejemplo de esto es el virus **DARK AVENGER**, que infecta archivos y acumula la cantidad de infecciones que realizó. Cuando este contador llega a 16, elige un sector del disco al azar y en él escribe la frase: "**Eddie lives somewhere in time**" (Eddie vive en algún lugar del tiempo).

Esto puede haber estado pasando por un largo tiempo sin que lo notemos, pero el día en que detectemos la presencia del virus y queramos restaurar el último backup notaremos que también él contiene sectores con la frase, y también los backups anteriores a ese.

Puede que lleguemos a encontrar un backup limpio, pero será tan viejo que muy probablemente hayamos perdido una gran cantidad de archivos que fueron creados con posterioridad a ese backup.

- **DAÑOS SEVEROS.**

Los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No sabemos cuándo los datos son correctos o han cambiado, pues no hay pistas obvias como en el caso del **DARK AVENGER** (es decir, no podemos buscar la frase **Eddie lives ...**).

- **DAÑOS ILIMITADOS.**

Algunos programas como **CHEEBA**, **VACSINA.44.LOGIN** y **GP1** entre otros, obtienen la clave del administrador del sistema y la pasan a un tercero. Cabe aclarar que estos no son virus sino troyanos. En el caso de **CHEEBA**, crea un nuevo usuario con los privilegios máximos, fijando el nombre del usuario y la clave. El daño es entonces realizado por la tercera persona, quien ingresará al sistema y haría lo que quisiera.

- **SÍNTOMAS TÍPICOS DE UNA INFECCIÓN.**

    - El sistema operativo o un programa toma mucho tiempo en cargar sin razón aparente.
    - El tamaño del programa cambia sin razón aparente.
    - El disco duro se queda sin espacio o reporta falta de espacio sin que esto sea necesariamente así.

- Si se corre el CHKDSK no muestra "655360 bytes available".
- En Windows aparece "32 bit error".
- La luz del disco duro en la CPU continua parpadeando aunque no se este trabajando ni haya protectores de pantalla activados. (Se debe tomar este síntoma con mucho cuidado, porque no siempre es así).
- No se puede "bootear" desde el Drive A, ni siquiera con los discos de rescate.
- Aparecen archivos de la nada o con nombres y extensiones extrañas.
- Suena "clicks" en el teclado (este sonido es particularmente aterrador para quien no esta advertido).
- Los caracteres de texto se caen literalmente a la parte inferior de la pantalla (especialmente en DOS).
- En la pantalla del monitor pueden aparecen mensajes absurdos tales como **"Tengo hambre. Introduce un Big Mac en el Drive A".**
- En el monitor aparece una pantalla con un fondo de cielo celeste, unas nubes blancas difuminadas, una ventana de vidrios repartidos de colores y una leyenda en negro que dice Windows '98 (No puedo evitarlo, es mas fuerte que yo...!!).

Una infección se soluciona con las llamadas "vacunas" (que impiden la infección) o con los remedios que desactivan y eliminan, (o tratan de hacerlo) a los virus de los archivos infectados. Hay cierto tipo de virus que no son desactivables ni removibles, por lo que se debe destruir el archivo infectado.

- **¿QUÉ ES UN ANTIVIRUS?.**

No para toda enfermedad existe cura, como tampoco existe una forma de erradicar todos y cada uno de los virus existentes.

Es importante aclarar que todo antivirus es un programa y que, como todo programa, sólo funcionará correctamente si es adecuado y está bien configurado. Además, un antivirus es una herramienta para el usuario y no sólo **no será eficaz para el 100% de los casos**, sino que **nunca será una protección total ni definitiva**.

La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independientemente de las prestaciones adicionales que pueda ofrecer, puesto que el hecho de detectar la posible presencia de un virus informático, detener el trabajo y tomar las medidas necesarias, es suficiente para acotar un buen porcentaje de los daños posibles. Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una entidad infectada.

El modelo más primario de las funciones de un programa antivirus es la detección de su presencia y, en lo posible, su identificación. La primera técnica que se popularizó para la detección de virus informáticos, y que todavía se sigue utilizando (aunque cada vez con menos eficiencia), es la técnica de **scanning**. Esta técnica consiste en revisar el código de todos los archivos contenidos en la unidad de almacenamiento −fundamentalmente los archivos ejecutables− en busca de pequeñas porciones de código que puedan pertenecer a un virus informático. Este procedimiento, denominado **escaneo**, se realiza a partir de una base de datos que contiene trozos de código representativos de cada virus conocido, agregando el empleo de determinados algoritmos que agilizan los procesos de búsqueda.

La técnica de **scanning** fue bastante eficaz en los primeros tiempos de los virus informáticos, cuando había pocos y su producción era pequeña. Este relativamente pequeño volumen de virus informáticos permitía que los desarrolladores de antivirus escaneadores tuvieran tiempo de analizar el virus, extraer el pequeño trozo de código que lo iba a identificar y agregarlo a la base de datos del programa para lanzar una nueva versión. Sin embargo, la obsolescencia de este mecanismo de identificación como una solución antivirus completa se encontró en su mismo modelo.

El primer punto grave de este sistema radica en que siempre brinda una solución *a posteriori*: es necesario que

un virus informático alcance un grado de dispersión considerable para que sea enviado (por usuarios capacitados, especialistas o distribuidores del producto) a los desarrolladores de antivirus. Estos lo analizarán, extraerán el trozo de código que lo identificará, y lo incluirán en la próxima versión de su programa antivirus. Este proceso puede demorar meses a partir del momento en que el virus comienza a tener una dispersión considerable, lapso en el cual puede causar graves daños sin que pueda ser identificado.

Además, **este modelo consiste en una sucesión infinita de soluciones parciales y momentáneas (cuya sumatoria jamás constituirá una solución definitiva)**, que deben actualizarse periódicamente debido a la aparición de nuevos virus.

En síntesis, la técnica de scanning es altamente ineficiente, pero se sigue utilizando debido a que permite identificar rápidamente la presencia de los virus más conocidos y, como son estos los de mayor dispersión, permite una importante gama de posibilidades.

Un ejemplo típico de un antivirus de esta clase es el **Viruscan de McAfee**, que se verá más adelante.

En virtud del pronto agotamiento técnico de la técnica de scanning, los desarrolladores de programas antivirus han dotado a sus creaciones de métodos para búsquedas de virus informáticos (y de sus actividades), que no identifican específicamente al virus sino a algunas de sus características generales y comportamientos universalizados.

Este tipo de método rastrea rutinas de alteración de información que no puedan ser controladas por el usuario, modificación de sectores críticos de las unidades de almacenamiento (master boot record, boot sector, FAT, entre otras), etc.

Un ejemplo de este tipo de métodos es el que utiliza algoritmos **heurísticos**.

De hecho, esta naturaleza de procedimientos busca, de manera bastante eficiente, códigos de instrucciones potencialmente pertenecientes a un virus informático. Resulta eficaz para la detección de virus conocidos y es una de las soluciones utilizadas por los antivirus para la detección de nuevos virus. El inconveniente que presenta este tipo de algoritmo radica en **que puede llegar a sospecharse de muchisimas cosas que no son virus**. Esto hace necesario que el usuario que lo utiliza conozca un poco acerca de la estructura del sistema operativo, a fin de poseer herramientas que le faciliten una discriminación de cualquier falsa alarma generada por un método heurístico.

Algunos de los antivirus de esta clase son F−Prot, Norton Anti Virus y Dr. Solomon's Toolkit.

Ahora bien, otra forma de detectar la presencia de un virus informático en un sistema consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar los sectores críticos de los dispositivos de almacenamiento o los archivos ejecutables. Los programas que realizan esta tarea se denominan **chequeadores de integridad**.

Sobre la base de estas consideraciones, podemos consignar que **un buen sistema antivirus** debe estar compuesto por **un programa detector de virus** −que siempre esté residente en memoria− y **un programa que verifique la integridad** de los sectores críticos del disco rígido y sus archivos ejecutables. Existen productos antivirus que cubren los dos aspectos, o bien pueden combinarse productos diferentes configurados de forma que no se produzcan conflictos entre ellos.

MODELO ANTIVIRUS:

La estructura de un programa antivirus, está compuesta por dos módulos principales: el primero denominado **de control** y el segundo denominado **de respuesta**. A su vez, cada uno de ellos se divide en varias partes:

- **Módulo de control:** posee la técnica **verificación de integridad** que posibilita el registro de cambios en los archivos ejecutables y las zonas críticas de un disco rígido. Se trata, en definitiva, de una herramienta preventiva para mantener y controlar los componentes de información de un disco rígido que no son modificados a menos que el usuario lo requiera.

Otra opción dentro de este módulo es la **identificación de virus**, que incluye diversas técnicas para la detección de virus informáticos. Las formas más comunes de detección son el scanning y los algoritmos, como por ejemplo, los heurísticos.

Asimismo, la **identificación de código dañino** es otra de las herramientas de detección que, en este caso, busca instrucciones peligrosas incluidas en programas, para la integridad de la información del disco rígido.

Esto implica descompilar (o desensamblar) en forma automática los archivos almacenados y ubicar sentencias o grupos de instrucciones peligrosas.

Finalmente, el módulo de control también posee una **administración de recursos** para efectuar un monitoreo de las rutinas a través de las cuales se accede al hardware de la computadora (acceso a disco, etc.). De esta manera puede limitarse la acción de un programa restringiéndole el uso de estos recursos, como por ejemplo impedir el acceso a la escritura de zonas críticas del disco o evitar que se ejecuten funciones de formato del mismo.

- **Módulo de respuesta:** la función **alarma** se encuentra incluida en todos los programas antivirus y consiste en detener la acción del sistema ante la sospecha de la presencia de un virus informático, e informar la situación a través de un aviso en pantalla.

Algunos programas antivirus ofrecen, una vez detectado un virus informático, la posibilidad de erradicarlo. Por consiguiente, la función **reparar** se utiliza como una solución momentánea para mantener la operatividad del sistema hasta que pueda instrumentarse una solución adecuada. Por otra parte, existen dos **técnicas para evitar el contagio de entidades ejecutables**: evitar que se contagie todo el programa o prevenir que la infección se expanda más allá de un ámbito fijo.

Aunque la primera opción es la más adecuada, plantea grandes problemas de implementación.

DETECCIÓN Y PREVENCIÓN.

Debido a que los virus informáticos son cada vez más sofisticados, hoy en día es difícil sospechar su presencia a través de síntomas como la pérdida de performance. De todas maneras la siguiente es una lista de síntomas que pueden observarse en una computadora de la que se sospeche esté infectada por alguno de los virus más comunes:

- Operaciones de procesamiento más lentas.
- Los programas tardan más tiempo en cargarse.
- Los programas comienzan a acceder por momentos a las disqueteras y/o al disco rígido.
- Disminución no justificada del espacio disponible en el disco rígido y de la memoria RAM disponible, en forma constante o repentina.
- Aparición de programas residentes en memoria desconocidos.

La primera medida de prevención a ser tenida en cuenta es, como se dijo anteriormente, contar con un sistema antivirus y utilizarlo correctamente. Por lo tanto, la única forma de que se constituya un bloqueo eficaz para un virus es que se utilice con determinadas normas y procedimientos. Estas normas tienden a controlar la entrada de archivos al disco rígido de la computadora, lo cual se logra revisando con el antivirus todos los disquetes o medios de almacenamiento en general y, por supuesto, disminuyendo al mínimo posible todo tipo

de tráfico.

Además de utilizar un sistema antivirus y controlar el tráfico de archivos al disco rígido, una forma bastante eficaz de **proteger los archivos ejecutables** es utilizar un programa **chequeador de integridad** que verifique que estos archivos no sean modificados, es decir, que mantengan su estructura. De esta manera, antes que puedan ser parasitados por un virus convencional, se impediría su accionar.

Para prevenir la infección con un **virus de sector de arranque**, lo más indicado es no dejar disquetes olvidados en la disquetera de arranque y contar con un antivirus. Pero, además, puede aprovecharse una característica que incorpora el setup de las computadoras más modernas: variar la secuencia de arranque de la PC a "**primero disco rígido y luego disquetera**" (C, A). De esta manera, la computadora no intentará leer la disquetera en el arranque aunque tenga cargado un disquete.

Algunos distribuidores o representantes de programas antivirus envían muestras de los nuevos virus argentinos a los desarrolladores del producto para que los estudien o incluyan en sus nuevas versiones o upgrades, con la demora que esto implica.

En consecuencia, la detección alternativa a la de scanning y las de chequeo de actividad e integridad resultan importantes, ya que pueden detectar la presencia de un virus informático sin la necesidad de identificarlo. Y esta es la única forma disponible para el usuario de detectar virus nuevos, sean nacionales o extranjeros.

De todas maneras, **existe una forma de actualizar la técnica de scanning**. La misma consiste en incorporarle al antivirus un archivo conteniendo cadenas de caracteres ASCII que sean trozos de código (strings) significativos del sector vital de cada nuevo virus que todavía no esté incorporado en la base de datos del programa.

De todas formas, esta solución será **parcial**: la nueva cadena introducida sólo *identificará* al virus, pero no será capaz de erradicarlo.

Es muy importante que los "strings" que se vayan a incorporar al antivirus provengan de una fuente confiable ya que, de lo contrario, pueden producirse falsas alarmas o ser ineficaces.

Algunos de los antivirus que soportan esta cualidad de *agregar* strings son Viruscan, F−Prot y Thunderbyte.

La NCSA (National Computer Security Association, Asociación Nacional de Seguridad de Computadoras) es la encargada de certificar productor antivirus.

Para obtener dicha certificación los productos deben pasar una serie de rigurosas pruebas diseñadas para asegurar la adecuada protección del usuario.

Antiguamente el esquema de certificación requería que se detectara (incluyendo el número de versión) el 90 % de la librería de virus del NCSA, y fue diseñado para asegurar óptimas capacidades de detección. Pero esta metodología no era completamente eficiente.

Actualmente, el esquema de certificación enfoca la amenaza a las computadoras empresariales. Para ser certificado, el producto debe pasar las siguientes pruebas:

- Debe detectar el 100% de los virus encontrados comúnmente. La lista de virus comunes es actualizada periódicamente, a medida que nuevos virus son descubiertos.
- Deben detectar, como mínimo, el 90% de la librería de virus del NCSA (más de 6.000 virus)

Estas pruebas son realizadas con el producto ejecutándose con su configuración "por defecto".

Una vez que un producto ha sido certificado, la NCSA tratará de recertificar el producto un mínimo de cuatro veces. Cada intento es realizado sin previo aviso al desarrollador del programa. Esta es una buena manera de asegurar que el producto satisface el criterio de certificación.

Si un producto no pasa la primera o segunda prueba, su distribuidor tendrá siete días para proveer de la corrección. Si este límite de tiempo es excedido, el producto será eliminado de la lista de productos certificados.

Una vez que se ha retirado la certificación a un producto la única forma de recuperarla es que el distribuidor envíe una nueva versión completa y certificable (no se aceptará sólo una reparación de la falla.

Acerca de la lista de virus de la NCSA, aclaremos que ningún desarrollador de antivirus puede obtener una copia. Cuando un antivirus falla en la detección de algún virus incluido en la lista, una cadena identificatoria del virus le es enviada al productor del antivirus para su inclusión en futuras versiones.

En el caso de los virus polimórficos, se incluyen múltiples copias del virus para asegurar que el producto testeado lo detecta perfectamente. Para pasar esta prueba el antivirus debe detectar cada mutación del virus.

La A. V. P. D. (Antivirus Product Developers, Desarrolladores de Productos Antivirus) es una asociación formada por las principales empresas informáticas del sector, entre las que se cuentan:

- Cheyenne Software
- I. B. M.
- Intel
- McAfee Associates
- ON Tecnology
- Stiller Research Inc.
- S&S International
- Symantec Corp.
- ThunderByte

- **ALGUNOS ANTIVIRUS.**

    - **DR. SOLOMON'S ANTIVIRUS TOOLKIT.**

Certificado por la NCSA. Detecta más de 6.500 virus gracias a su propio lenguaje de detección llamado **VirTran**, con una velocidad de detección entre 3 y 5 veces mayor que los antivirus tradicionales.

Uno de los últimos desarrollos de S&S es la tecnología G. D. E. (Generic Decription Engine, Motor de Desencriptación Genérica) que permite detectar virus polimórficos sin importar el algoritmo de encriptación utilizado.

Permite detectar modificaciones producidas tanto en archivos como en la tabla de partición del disco rígido. Para ello utiliza Checksumms Criptográficos lo cual, sumado a una clave personal de cada usuario, hace casi imposible que el virus pueda descubrir la clave de encriptación.

Elimina virus en archivos en forma sencilla y efectiva con pocas falsas alarmas, y en sectores de buteo y tablas de partición la protección es genérica, es decir, independiente del virus encontrado.

Otras características que presenta este antivirus, son:

- Ocupa 9K de memoria extendida o expandida.

- Documentación amplia y detallada en español y una enciclopedia sobre los virus más importantes.
- Actualizaciones mensuales o trimestrales de software y manuales.
- Trabaja como residente bajo Windows.
- A. H. A. (Advanced Heuristic Analysis, Análisis Heurístico Avanzado).
- **NORTON ANTIVIRUS.**

Certificado por la NCSA. Posee una protección automática en segundo plano. Detiene prácticamente todos los virus conocidos y desconocidos (a través de una tecnología propia denominada **NOVI**, que implica control de las actividades típicas de un virus, protegiendo la integridad del sistema), antes de que causen algún daño o pérdida de información, con una amplia línea de defensa, que combina búsqueda, detección de virus e **inoculación** (se denomina 'inoculación' al método por el cual este antivirus toma las características principales de los sectores de booteo y archivos para luego chequear su integridad. Cada vez que se detecta un cambio en dichas áreas, NAV avisa al usuario y provee las opciones de Reparar − Volver a usar la imagen guardada − Continuar − No realiza cambios − Inocular − Actualizar la imagen.

Utiliza diagnósticos propios para prevenir infecciones de sus propios archivos y de archivos comprimidos.

El escaneo puede ser lanzado manualmente o automáticamente a través de la planificación de fecha y hora. También permite reparar los archivos infectados por virus desconocidos. Incluye información sobre muchos de los virus que detecta y permite establecer una contraseña para aumentar así la seguridad.

La lista de virus conocidos puede ser actualizada periódicamente (sin cargo) a través de servicios en línea como Internet, América On Line, Compuserve, The Microsoft Network o el BBS propio de Symantec, entre otros.

- **VIRUSSCAN.**

Este antivirus de **McAfee Associates** es uno de los más famosos. Trabaja por el sistema de scanning descripto anteriormente, y es el mejor en su estilo.

Para escanear, hace uso de dos técnicas propias: CMS (Code Matrix Scanning, Escaneo de Matriz de Código) y CTS (Code Trace Scanning, Escaneo de Seguimiento de Código).

Una de las principales ventajas de este antivirus es que la actualización de los archivos de bases de datos de strings es muy fácil de realizar, lo cual, sumado a su condición de programa shareware, lo pone al alcance de cualquier usuario. Es bastante flexible en cuanto a la configuración de cómo detectar, reportar y eliminar virus.

- **CONCLUSIONES.**

En razón de lo expresado pueden extraerse algunos conceptos que pueden considerarse necesarios para tener en cuenta en materia de virus informáticos:

- No todo lo que afecte el normal funcionamiento de una computadora es un virus.
- **TODO** virus es un programa y, como tal, debe ser ejecutado para activarse.
- Es imprescindible contar con herramientas de detección y desinfección.
- **NINGÚN** sistema de seguridad es 100% seguro. Por eso todo usuario de computadoras debería tratar de implementar estrategias de seguridad antivirus, no sólo para proteger su propia información sino para no convertirse en un agente de dispersión de algo que puede producir daños graves e indiscriminados.

Para implementar tales estrategias deberían tenerse a mano los siguientes elementos:

- **UN DISCO DE SISTEMA PROTEGIDO CONTRA ESCRITURA Y LIBRE DE VIRUS:** Un disco que contenga el sistema operativo ejecutable (es decir, que la máquina pueda ser arrancada desde este disco) con protección contra escritura y que contenga, por lo menos, los siguientes comandos: FORMAT, FDISK, MEM y CHKDSK (o SCANDISK en versiones recientes del MS−DOS).
- **POR LO MENOS UN PROGRAMA ANTIVIRUS ACTUALIZADO:** Se puede considerar actualizado a un antivirus que no tiene más de tres meses desde su fecha de creación (o de actualización del archivo de strings). Es muy recomendable tener por lo menos dos antivirus.
- **UNA FUENTE DE INFORMACIÓN SOBRE VIRUS ESPECÍFICOS:** Es decir, algún programa, libro o archivo de texto que contenga la descripción, síntomas y características de por lo menos los cien virus más comunes.
- **UN PROGRAMA DE RESPALDO DE ÁREAS CRÍTICAS:** Algún programa que obtenga respaldo (backup) de los sectores de arranque de los disquetes y sectores de arranque maestro (MBR, Master Boot Record) de los discos rígidos. Muchos programas antivirus incluyen funciones de este tipo.
- **LISTA DE LUGARES DÓNDE ACUDIR:** Una buena precaución es no esperar a necesitar ayuda para comenzar a buscar quién puede ofrecerla, sino ir elaborando una agenda de direcciones, teléfonos y direcciones electrónicas de las personas y lugares que puedan servirnos más adelante. Si se cuenta con un antivirus comercial o registrado, deberán tenerse siempre a mano los teléfonos de soporte técnico.
- **UN SISTEMA DE PROTECCIÓN RESIDENTE:** Muchos antivirus incluyen programas residentes que previenen (en cierta medida), la intrusión de virus y programas desconocidos a la computadora.
- **TENER RESPALDOS:** Se deben tener respaldados en disco los archivos de datos más importantes, además, se recomienda respaldar todos los archivos ejecutables. Para archivos muy importantes, es bueno tener un respaldo doble, por si uno de los discos de respaldo se daña. Los respaldos también pueden hacerse en cinta (tape backup), aunque para el usuario normal es preferible hacerlo en discos, por el costo que las unidades de cinta representan.
- **REVISAR TODOS LOS DISCOS NUEVOS ANTES DE UTILIZARLOS:** Cualquier disco que no haya sido previamente utilizado debe ser revisado, inclusive los programas originales (pocas veces sucede que se distribuyan discos de programas originales infectados, pero es factible) y los que se distribuyen junto con revistas de computación.
- **REVISAR TODOS LOS DISCOS QUE SE HAYAN PRESTADO:** Cualquier disco que se haya prestado a algún amigo o compañero de trabajo, aún aquellos que sólo contengan archivos de datos, deben ser revisados antes de usarse nuevamente.
- **REVISAR TODOS LOS PROGRAMAS QUE SE OBTENGAN POR MÓDEM O REDES:** Una de las grandes vías de contagio la constituyen Internet y los BBS, sistemas en los cuales es común la transferencia de archivos, pero no siempre se sabe desde dónde se está recibiendo información.
- **REVISAR PERIÓDICAMENTE LA COMPUTADORA:** Se puede considerar que una buena frecuencia de análisis es, por lo menos, mensual.

Finalmente, es importante tener en cuenta estas sugerencias referentes al comportamiento a tener en cuenta frente a diferentes situaciones:

- Cuando se va a revisar o desinfectar una computadora, es conveniente apagarla por más de 5 segundos y arrancar desde un disco con sistema, libre de virus y protegido contra escritura, para eliminar virus residentes en memoria. No se deberá ejecutar ningún programa del disco rígido, sino que el antivirus deberá estar en el disquete. De esta manera, existe la posibilidad de detectar virus stealth.
- Cuando un sector de arranque (boot sector) o de arranque maestro (MBR) ha sido infectado, es preferible restaurar el sector desde algún respaldo, puesto que en ocasiones, los sectores de arranque genéricos utilizados por los antivirus no son perfectamente compatibles con el sistema operativo instalado. Además, los virus no siempre dejan un respaldo del sector original donde el antivirus espera

encontrarlo.

- Antes de restaurar los respaldos es importante no olvidar apagar la computadora por más de cinco segundos y arrancar desde el disco libre de virus.
- Cuando se encuentran archivos infectados, es preferible borrarlos y restaurarlos desde respaldos, aún cuando el programa antivirus que usemos pueda desinfectar los archivos. Esto es porque no existe seguridad sobre si el virus detectado es el mismo para el cual fueron diseñadas las rutinas de desinfección del antivirus, o es una mutación del original.
- Cuando se va a formatear un disco rígido para eliminar algún virus, debe recordarse apagar la máquina por más de cinco segundos y posteriormente arrancar el sistema desde nuestro disquete limpio, donde también debe encontrarse el programa que se utilizará para dar formato al disco.
- Cuando, por alguna causa, no se puede erradicar un virus, deberá buscarse la asesoría de un experto directamente pues, si se pidiera ayuda a cualquier aficionado, se correrá el riesgo de perder definitivamente datos si el procedimiento sugerido no es correcto.
- Cuando se ha detectado y erradicado un virus es conveniente reportar la infección a algún experto, grupo de investigadores de virus, soporte técnico de programas antivirus, etc. Esto que en principio parecería innecesario, ayuda a mantener estadísticas, rastrear focos de infección e identificar nuevos virus, lo cual en definitiva, termina beneficiando al usuario mismo.