1 Introducción

Los virus informáticos han ocasionado fuertes problemas a lo largo de la historia de las computadoras. En un comienzo estos eran tan poco habituales que no se les consideraba un virus, se pensaba que podría ser un error en un programa pero la evolución de los virus ha ocasionado que estos fueran mas sofisticados lo que motivo a varios desarrolladores a crear una herramientas la que hoy s le conoce como antivirus.

Hoy en día los virus han dejado de evolucionar, se encargan principalmente de robar información u obtener dinero ilícitamente tomando control de cuentas bancarias, por poner un ejemplo. La mayoría de las personas se ha topado alguna vez con este tipo de malware y le ha ocasionado bastantes problemas como la perdida de archivos como tareas o fotos simplemente ralentizando su computadora. Esto puede evitarse si las personas consiguieran un software antivirus de calidad y mantengan actualizada su base de datos, aun así mucha gente desconoce que su computadora puede ser vulnerable a los virus o simplemente no les importa que su ordenador se infecte.

1.1 Objetivos generales

Con este trabajo voy a demostrar los efectos que pueden provocar los virus en las computadoras, cuales tipos de virus hay, que son y como prevenirlos, también demostrare lo que es un software antivirus y cuales son sus funciones.

1.2 Objetivos específicos

Explicar el funcionamiento de los virus, sus tipos y su historia desde sus orígenes hasta las fechas donde su evolución se freno.

1.3 Justificación

Este proyecto lo realizo para mostrar a la gente que los virus pueden y deben ser prevenidos, también para explicar su funcionamiento, la variedad que estos presentan y como podemos evitarlos haciendo uso de un software antivirus.

2 Virus Informático [1]

Es un programa informático diseñado para infectar archivos. Además, algunos podrían ocasionar efectos molestos, destructivos e incluso irreparables en los sistemas sin el consentimiento y/o conocimiento del usuario.

Cuando se introduce en un sistema normalmente se alojará dentro del código de otros programas. El virus no actúa hasta que no se ejecuta el programa infectado. Algunos de ellos, además están preparados para activarse cuando se cumple una determinada condición (una fecha concreta, una acción que realiza el usuario, etc.).

El término virus informático se debe a su enorme parecido con los virus biológicos. Del mismo modo que los virus biológicos se introducen en el cuerpo humano e infectan una célula, que a su vez infectará nuevas células, los virus informáticos se introducen en los ordenadores e infectan ficheros insertando en ellos su código. Cuando el programa infectado se ejecuta, el código entra en funcionamiento y el virus sigue extendiéndose.

2.1 ¿Qué hacen los Virus Informáticos?

Los efectos de los virus pueden ser muy molestos para los usuarios ya que la infección de un fichero puede provocar la ralentización del ordenador o la modificación en su comportamiento y funcionamiento, entre otras cosas.

Los objetivos de los virus suelen ser los programas ejecutables (ficheros con extensión .EXE o .COM). Sin embargo, también pueden infectar otros tipos de ficheros, como páginas Web (.HTML), documentos de Word (.DOC), hojas de cálculo XLS), etc.

Los virus se pueden clasificar en función de múltiples características y criterios: según su funcionalidad, las técnicas que utilizan para infectar, los tipos de ficheros que infectan, los lugares donde se alojan, el sistema operativo o la plataforma tecnológica que atacan, etc.

2.2 Significado [2]

La palabra VIRUS es el acrónimo de Vital Information Resources Under Siege que en español significa "Recursos Informáticos Vitales Bajo Riesgo", aunque se adaptó este acrónimo debido a que la forma de "funcionamiento" de este tipo de programas es muy similar a los virus biológicos, ya que ambos necesitan un lugar para alojarse y desde ahí disparar su efecto.

3 Historia [3]

1949: el famoso científico matemático John Louis Von Neumann, de origen húngaro, escribió un artículo, publicado en una revista científica de New York, exponiendo su "Teoría y organización de autómatas complejos", donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura.

1959: en los laboratorios de la Bell Computer, subsidiaria de AT &
T, 3 jóvenes programadores: Robert Thomas Morris, Douglas McIlory y Victor Vysottsky, a manera de entretenimiento crearon un juego al que denominaron CoreWar, inspirados en la teoría de John Von Neumann, escrita y publicada en 1949.

Puesto en la práctica, los contendores del CoreWar ejecutaban programas que iban paulatinamente disminuyendo la memoria del computador y el ganador era el que finalmente conseguía eliminarlos totalmente. Este juego fue motivo de concursos en importantes centros de investigación como el de la Xerox en California y el Massachussets Technology Institute (MIT), entre otros. Sin embargo, durante muchos años el CoreWar fue mantenido en el anonimato, debido a que por aquellos años la computación era manejada por una pequeña élite de intelectuales.

1872: Existen reportes acerca del virus Creeper, creado por Robert Thomas Morris, que atacaba a las IBM 360, emitiendo periódicamente en la pantalla el mensaje: "I'm a creeper... catch me if you can!" (soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (segadora), ya que por aquella época se desconocía el concepto de software antivirus.

1980: La red ArpaNet del ministerio de Defensa de los Estados Unidos de América, precursora de Internet, emitió extraños mensajes que aparecían y desaparecían en forma aleatoria, asimismo algunos códigos ejecutables de los programas usados sufrían una mutación. Los altamente calificados técnicos del Pentágono se demoraron 3 largos días en desarrollar el programa

antivirus correspondiente. Hoy día los desarrolladores de antivirus resuelven un problema de virus en contados minutos.

Agosto de 1981: La International Business Machine lanza al mercado su primera computadora personal, simplemente llamada IBM PC. Un año antes, la IBM habían buscado infructuosamente a Gary Kildall, de la Digital Research, para adquirirle los derechos de su sistema operativo CP/M, pero éste se hizo de rogar, viajando a Miami donde ignoraba las continuas llamadas de los ejecutivos del "gigante azul".

Es cuando oportunamente surge Bill Gates, de la Microsoft Corporation y adquiere a la Seattle Computer Products, un sistema operativo desarrollado por Tim Paterson, que realmente era un "clone" del CP/M. Gates le hizo algunos ligeros cambios y con el nombre de PC-DOS se lo vendió a la IBM. Sin embargo, Microsoft retuvo el derecho de explotar dicho sistema, bajo el nombre de MS-DOS.

El nombre del sistema operativo de Paterson era "Quick and Dirty DOS" (Rápido y Rústico Sistema Operativo de Disco) y tenía varios errores de programación (bugs).

La enorme prisa con la cual se lanzó la IBM PC impidió que se le dotase de un buen sistema operativo y como resultado de esa imprevisión todas las versiones del llamado PC-DOS y posteriormente del MS-DOS fueron totalmente vulnerables a los virus, ya que fundamentalmente heredaron muchos de los conceptos de programación del antiguo sistema operativo CP/M, como por ejemplo el PSP (Program Segment Prefix), una rutina de apenas 256 bytes, que es ejecutada previamente a la ejecución de cualquier programa con extensión EXE o COM.

1983: Keneth Thompson, quien en 1969 creó el sistema operativo UNIX, resucitó las teorías de Von Neumann y la de los tres programadores de la Bell y en 1983 siendo protagonista de una ceremonia pública presentó y demostró la forma de desarrollar un virus informático.

1984: Fred Cohen al año siguiente, el Dr. Fred Cohen al ser homenajeado en una graduación, en su discurso de agradecimiento incluyó las pautas para el desarrollo de un virus. Este y otros hechos posteriores lo convirtieron en el primer autor oficial de los virus, aunque hubo varios autores más que actuaron en el anonimato.

El Dr. Cohen ese mismo año escribió su libro "Virus informáticos: teoría y experimentos", donde además de definirlos los califica como un grave problema relacionado con la Seguridad Nacional. Posteriormente este investigador escribió "El evangelio según Fred" (The Gospel according to Fred), desarrolló varias especies virales y experimentó con ellas en un computador VAX 11/750 de la Universidad de California del Sur.

La verdadera voz de alarma se dio en 1984 cuando los usuarios del BIX BBS de la revista BYTE reportaron la presencia y difusión de algunos programas que actuaban como "caballos de troya", logrando infectar a otros programas. Al año siguiente los mensajes y quejas se incrementaron y fue en 1986 que se reportaron los primeros virus conocidos que ocasionaron serios daños en las IBM PC y sus clones.

1986: El comienzo de la gran epidemia ese año se difundieron los virus (c) Brain, Bouncing Ball y Marihuana y que fueron las primeras especies representativas de difusión masiva. Estas 3 especies virales tan sólo infectaban el sector de arranque de los disquetes. Posteriormente aparecieron los virus que infectaban los archivos con extensión EXE y COM.

2 de noviembre de 1988: Robert Tappan Morris, hijo de uno de los precursores de los virus y recién graduado en Computer Science en la Universidad de Cornell, difundió un virus a través de ArpaNet, (precursora de Internet) logrando infectar 6,000 servidores conectados a la red.

Mediados de 1995: se reportaron en diversas ciudades del mundo la aparición de una nueva familia de virus que no solamente infectaban documentos, sino que, a su vez, sin ser archivos ejecutables podían auto-copiarse infectando a otros documentos. Los llamados macro virus tan sólo infectaban a los archivos de MS-Word, posteriormente apareció una especie que atacaba al Ami Pro, ambos procesadores de textos.

1997: Se disemina a través de Internet el primer macro virus que infecta hojas de cálculo de MS-Excel, denominado Laroux, y en 1998 surge otra especie de esta misma familia de virus que ataca a los archivos de bases de datos de MS-Access

Principios de 1999: se empezaron a propagar masivamente en Internet los virus anexados (adjuntos) a mensajes de correo, como el Melisa o el macro virus Papa. Ese mismo año fue difundido a través de Internet el peligroso CIH y el ExploreZip, entre otros muchos más.

Fines de noviembre de 1999: apareció el BubbleBoy, primer virus que infectaba los sistemas con tan sólo leer el mensaje de correo, el mismo que se muestra en formato HTML.

Junio del 2000: se reportó el VBS/Stages.SHS, primer virus oculto dentro del shell de la extensión .SHS.

2002: Surge el primer virus diseñado para atacar archivos Shockwave Flash de Macromedia y aparece winux, primer virus para ejecutables tanto de Windows como de Linux.

4 Tipos de virus [4]

Los virus se pueden clasificar en función de múltiples características y criterios: según su origen, las técnicas que utilizan para infectar, los tipos de ficheros que infectan, los lugares donde se esconden, los daños que causan, el sistema operativo o la plataforma tecnológica que atacan, etc.

Todas estas clasificaciones tienen muchos puntos en común, por lo que un mismo virus puede pertenecer a varias categorías al mismo tiempo. Por otro lado, continuamente surgen nuevos virus que por su reciente aparición o por sus peculiares características no pueden ser incluidos inicialmente en ninguna categoría, aunque esto no es lo habitual.

4.1 Virus residentes

La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados, etc. Estos virus sólo atacan cuando se cumplen ciertas condiciones definidas previamente por su creador (por ejemplo, una fecha y hora determinada). Mientras tanto, permanecen ocultos en una zona de la memoria principal, ocupando un espacio de la misma, hasta que son detectados y eliminados.

4.2 Virus de acción directa

Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos.

Además, también realizan sus acciones en los directorios especificados dentro de la línea PATH (camino o ruta de directorios), dentro del fichero AUTOEXEC.BAT (fichero que siempre se encuentra en el directorio raíz del disco duro). Los virus de acción directa presentan la ventaja de que los ficheros afectados por ellos pueden ser desinfectados y restaurados completamente.

4.3 Virus de sobreescritura

Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.

También se diferencian porque los ficheros infectados no aumentan de tamaño, a no ser que el virus ocupe más espacio que el propio fichero (esto se debe a que se colocan encima del fichero infectado, en vez de ocultarse dentro del mismo). La única forma de limpiar un fichero infectado por un virus de sobreescritura es borrarlo, perdiéndose su contenido.

4.4 Virus de boot o de arranque

Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco (tanto un disquete como un disco duro respectivamente). En ella se guarda la información esencial sobre las características del disco y se encuentra un programa que permite arrancar el ordenador.

Este tipo de virus no infecta ficheros, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los disquetes. Cuando un ordenador se pone en marcha con un disquete infectado, el virus de boot infectará a su vez el disco duro. Los virus de boot no pueden afectar al ordenador mientras no se intente poner en marcha a éste último con un disco infectado. Por tanto, el mejor modo de defenderse contra ellos es proteger los disquetes contra escritura y no arrancar nunca el ordenador con un disquete desconocido en la disquetera.

4.5 Virus de macro

El objetivo de estos virus es la infección de los ficheros creados usando determinadas aplicaciones que contengan macros: documentos de Word (ficheros con extensión DOC), hojas de cálculo de Excel (ficheros con extensión XLS), bases de datos de Access (ficheros con extensión MDB), presentaciones de PowerPoint (ficheros con extensión PPS), ficheros de Corel Draw, etc.

Las macros son micro-programas asociados a un fichero, que sirven para automatizar complejos conjuntos de operaciones. Al ser programas, las macros pueden ser infectadas.

Cuando se abre un fichero que contenga un virus de este tipo, las macros se cargarán de forma automática, produciéndose la infección. La mayoría de las aplicaciones que utilizan macros cuentan con una protección antivirus y de seguridad específica, pero muchos virus de

macro sortean fácilmente dicha protección.

Existe un tipo diferente de virus de macro según la herramienta usada: de Word, de Excel, de Access, de PowerPoint, multiprograma o de archivos RTF. Sin embargo, no todos los programas o herramientas con macros pueden ser afectadas por estos virus.

4.6 Virus de enlace o directorio

Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.

Los virus de enlace o directorio alteran las direcciones que indican donde se almacenan los ficheros. De este modo, al intentar ejecutar un programa (fichero con extensión EXE o COM) infectado por un virus de enlace, lo que se hace en realidad es ejecutar el virus, ya que éste habrá modificado la dirección donde se encontraba originalmente el programa, colocándose en su lugar.

Una vez producida la infección, resulta imposible localizar y trabajar con los ficheros originales.

4.7 Virus encriptados

Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran o encriptan a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.

4.8 Virus polimórficos

Son virus que en cada infección que realizan se cifran o encriptan de una forma distinta (utilizando diferentes algoritmos y claves de cifrado).

De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.

4.9 Virus multipartites

Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.

Se consideran muy peligrosos por su capacidad de combinar muchas técnicas de infección y por los dañinos efectos de sus acciones.

4.10 Virus de fichero

Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.

La mayoría de los virus existentes son de este tipo.

4.11 Virus de compañía

Son virus de fichero que al mismo tiempo pueden ser residentes o de acción directa. Su nombre deriva de que "acompañan" a otros ficheros existentes en el sistema antes de su llegada, sin modificarlos como hacen los virus de sobrescritura o los residentes.

Para efectuar las infecciones, los virus de compañía pueden esperar ocultos en la memoria hasta que se lleve a cabo la ejecución de algún programa, o actuar directamente haciendo copias de sí mismos.

4.12 Virus de FAT

La Tabla de Asignación de Ficheros o FAT es la sección de un disco utilizado para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema.

Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador. Los daños causados a la FAT se traducirán en pérdidas de la información contenida en ficheros individuales y en directorios completos.

4.13 Gusanos (Worms)

De un modo estricto, los gusanos no se consideran virus porque no necesitan infectar otros ficheros para reproducirse. A efectos prácticos, son tratados como virus y son detectados y eliminados por los antivirus.

Básicamente, los gusanos se limitan a realizar copias de sí mismos a la máxima velocidad posible, sin tocar ni dañar ningún otro fichero. Sin embargo, se reproducen a tal velocidad que pueden colapsar por saturación las redes en las que se infiltran.

Las infecciones producidas por estos virus casi siempre se realizan a través del correo electrónico, las redes informáticas y los canales de Chat (tipo IRC o ICQ) de Internet. También pueden propagarse dentro de la memoria del ordenador.

4.14 Troyanos o caballos de Troya

Técnicamente, los Troyanos tampoco se consideran virus, ya que no se reproducen infectando otros ficheros. Tampoco se propagan haciendo copias de sí mismo como hacen los gusanos. A efectos prácticos, son tratados como virus y son detectados y eliminados por los antivirus.

El objetivo básico de estos virus es la introducción e instalación de otros programas en el ordenador, para permitir su control remoto desde otros equipos.

Su nombre deriva del parecido en su forma de actuar de los astutos griegos de la mitología: llegan al ordenador como un programa aparentemente inofensivo. Sin embargo, al ejecutarlo instalará en nuestro ordenador un segundo programa, el troyano.

Los efectos de los Troyanos pueden ser muy peligrosos. Al igual que los virus, tienen la capacidad de eliminar ficheros o destruir la información del disco duro. Pero además pueden capturar y reenviar datos confidenciales a una dirección externa o abrir puertos de comunicaciones, permitiendo que un posible intruso controle nuestro ordenador de forma remota.

4.15 Bombas lógicas

Tampoco se consideran estrictamente virus, ya que no se reproducen. Ni siquiera son programas independientes, sino un segmento camuflado dentro de otro programa.

Tienen por objetivo destruir los datos de un ordenador o causar otros daños de consideración en él cuando se cumplen ciertas condiciones. Mientras este hecho no ocurre, nadie se percata de la presencia de la bomba lógica. Su acción puede llegar a ser tremendamente destructiva.

4.16 Virus falsos

Al margen de las divisiones anteriores, existen ciertos tipos de mensajes o programas que en ciertos casos son confundidos con virus, pero que no son virus en ningún sentido.

El principal componente de este grupo son los hoaxes o bulos. Los hoaxes no son virus, sino mensajes de correo electrónico engañosos, que se difunden masivamente por Internet sembrando la alarma sobre supuestas infecciones víricas y amenazas contra los usuarios. Los hoaxes tratan de ganarse la confianza de los usuarios aportando datos que parecen ciertos y proponiendo una serie de acciones a realizar para librarse de la supuesta infección.

Si se recibe un hoax, no hay que hacer caso de sus advertencias e instrucciones: lo más aconsejable es borrarlo sin prestarle la más mínima atención y no reenviarlo a otras personas.

5 Ejemplo de un virus [5]

Uno de los virus más peligrosos de los ultimos tiempos I LOVE YOU

El proceso. La infección comienza cuando un usuario recibe un correo electrónico titulado I Love You (Te quiero), que lleva asociado un fichero llamado LOVE-LETTER-FOR-YOU.TXT.vbs. (Carta de amor para ti). Este último archivo contiene el código del virus, supuestamente firmado con el apodo spyder (araña), fechado en Manila (Filipinas) e incluye una expeditiva frase I hate go to school (Odio ir al colegio).

A diferencia de su predecesor, el virus Melissa, que elegía las primeras 50 direcciones de la agenda del usuario para enviar una copia del virus, I love you toma todas las direcciones, lo cual aumenta su capacidad de reproducción.

Aquellas personas cuya dirección de correo electrónico figuren en la agenda del ordenador infectado recibirán en su buzón electrónico una copia del virus I love you, y si alguno de estos destinatarios decide abrir el mensaje, el proceso se repetirá provocando que la expansión del virus siga una progresión geométrica.

I love you se instala en el ordenador y borra ficheros de gráficos y de sonido -extensiones JPG, JPEG, MP3 y MP2-, sustituyéndolos por otros con el mismo nombre y la extensión VBS e introduciendo el código malicioso.

6 Métodos que utilizan los virus para propagarse [6]

1.- Añadidura o empalme Un virus usa el sistema de infección por añadidura cuando agrega el código vírico al final de los archivos ejecutables. Los archivos ejecutables anfitriones son mod-

ificados para que, cuando se ejecuten, el control del programa se pase primero al código vírico añadido. Esto permite que el virus ejecute sus tareas específicas y luego entregue el control al programa. Esto genera un incremento en el tamaño del archivo lo que permite su fácil detección.

2.- Inserción Un virus usa el sistema de infección por inserción cuando copia su código directamente dentro de archivos ejecutables, en vez de añadirse al final de los archivos anfitriones. Copian su código de programa dentro de un código no utilizado o en sectores marcados como dañados dentro del archivo por el sistema operativo con esto evita que el tamaño del archivo varíe. Para esto se requieren técnicas muy avanzadas de programación, por lo que no es muy utilizado este método.

3.- Reorientación Es una variante del anterior. Se introduce el código principal del virus en zonas físicas del disco rígido que se marcan como defectuosas y en los archivos se implantan pequeños trozos de código que llaman al código principal al ejecutarse el archivo. La principal ventaja es que al no importar el tamaño del archivo el cuerpo del virus puede ser bastante importante y poseer mucha funcionalidad. Su eliminación es bastante sencilla, ya que basta con reescribir los sectores marcados como defectuosos.

4.- Polimorfismo Este es el método mas avanzado de contagio. La técnica consiste en insertar el código del virus en un archivo ejecutable, pero para evitar el aumento de tamaño del archivo infectado, el virus compacta parte de su código y del código del archivo anfitrión, de manera que la suma de ambos sea igual al tamaño original del archivo. Al ejecutarse el programa infectado, actúa primero el código del virus descompactando en memoria las porciones necesarias. Una variante de esta técnica permite usar métodos de encriptación dinámicos para evitar ser detectados por los antivirus.

5.- Sustitución Es el método mas tosco. Consiste en sustituir el código original del archivo por el del virus. Al ejecutar el archivo deseado, lo único que se ejecuta es el virus, para disimular este proceder reporta algún tipo de error con el archivo de forma que creamos que el problema es del archivo.

7 Formas de contagio[7]

El contagio de un virus puede darse mediante el intercambio de dispositivos de almacenamiento como son los disquetes y discos compactos provenientes de fuentes sospechosas o desconocidas. También es posible contraer una infección al abrir un archivo adjunto (ya sean documentos, hojas de cálculo, archivos ejecutables, imágenes, etc.) contenido en un correo electrónico. Hoy en día, los virus se distribuyen además en las populares redes Peer-to-Peer que son aquellas utilizadas para distribuir software, música, videos, etc.

8 Efectos que causan los virus en el PC[8]

• Su computadora funciona más lenta de lo normal.
• Su computadora se congela, se cuelga o no responde.
• Existen nuevos iconos en su escritorio que usted no reconoce.
• Su computadora se reinicia por si sola (no se reinicia por actualizaciones de Windows Update)
• Aparecen mensajes inusuales de error (por ejemplo, mensajes de pérdida o corrupción de archivos o carpetas)

• No puede acceder al Panel de Control, Administrador de Tareas, Editor de Registro o Símbolo del sistema.

9 Prevenir los virus informáticos [9]

1. Instale un buen y confiable Antivirus: Actualizándolo diariamente o cada vez que hubiera actualizaciones disponibles. Estas deben tener vacunas en tiempo real (evitara el acceso de virus en tiempo real) y protecciones heurísticas.

2. Utilizar un Sistema Operativo seguro: Gran porcentaje de los virus tienen como objetivo atacar a los sistemas operativos de Microsoft por ser los más utilizados por los usuarios (o los más vulnerables). Las versiones de Windows diseñadas para el mercado doméstico son especialmente vulnerables, por lo que se recomienda utilizar los que tengan gestión de usuarios, permisos, seguridad, etc., como Windows 2000, Windows 7 (teniendo activado el 'Control de cuentas de usuario'), etc.

3. Evite instalar programas desconfiables o inseguros: No descargue programas que desconoce y que no sepa si son seguros. También evite utilizar programas P2P (programa de descarga de música, videos, etc.) como Ares, eMule, entre otros.

4. Ejecute Windows Update: Es una herramienta de Microsoft que ayuda a parchar su sistema operativo con el fin de evitar ataques virales o de hackers producto de vulnerabilidades. Puede descargar estos parches desde la web oficial de "Windows Update" en el siguiente enlace: www.windowsupdate.com. En algunos Sistemas Operativos como Windows 7/Vista/XP las actualizaciones son automáticas previa configuración del "Centro de Seguridad" en el "Panel de Control".

5. No abra archivos adjuntos por correo, chat, etc.: No abra ni ejecute archivos de personas que usted desconozca o que no haya pedido.

6. No arranque desde un disco flexible o USB: Retire cualquier disco flexible (disquete) o USB cuando inicie el ordenador.

7. Ponga contraseñas a su ordenador: Establezca contraseñas seguras tanto para el acceso a su sistema operativo como para sus carpetas compartidas (solo lectura), de preferencia estas deben tener caracteres especiales (ejemplo: R3nz0, Pctov4r, etc.).

8. No visite webs de hackeo, adultos, casinos online o de dudosa procedencia: Cuando usted visita páginas webs sospechosas es probable que estas intenten instalar o ejecutar en su ordenador algunos componentes peligrosos (ActiveX, scripts, etc.) con la finalidad de acceder a su ordenador o instalar un programa espía. También se recomienda no aceptar 'avisos' o 'certificados' ya que puede abrir las "puertas" de su PC hacia un ataque inminente.

9. Instalar un programa cortafuegos (Firewall): Los Firewalls son un buen mecanismo de seguridad contra ataques que provienen de Internet/Red, estos evitan intrusiones hacia nuestro ordenador o el robo de información. Actualmente varios antivirus ya vienen con firewall.

10. No permita utilizar su PC a otras personas: Si presta su ordenador a otras personas, no sabrá lo que hacen o lo que instalan y es probable que lo infecten.

11. Un programa 'Congelador' (opcional): Puede utilizar un programa 'congelador' que evita que se graben cualquier archivo, programa o 'virus' en su ordenador.

10 Antivirus [10]

Un antivirus es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

11 Como funcionan: [11]

El software antivirus analiza archivos en busca de ciertos patrones que puedan indicar una infección por malware, aunque los detalles varían entre los distintos paquetes. Los patrones que busca se basan en firmas o definiciones de virus conocidos. Los creadores de virus constantemente crean nuevos virus o actualizan los ya existentes, por tal motivo es importante instalar las últimas definiciones de virus en tu equipo.

Una vez que hayas instalado un paquete antivirus en tu equipo, es importante que realices un análisis o escaneo completo de forma periódica.

La mayoría del software antivirus permite realizar dos tipos de escaneos en un equipo de cómputo:

Escaneos automáticos: Dependiendo del software que se haya elegido, es posible configurarlo de forma que automáticamente analice archivos o carpetas específicas oprogramarlo para que ejecute un análisis completo del equipo en ciertos intervalos de tiempo.

Escaneos manuales: También, es una buena recomendación escanear archivos que se reciben de fuentes externas antes de abrirlos. Esto incluye:

Archivos adjuntos de correos electrónicos o archivos descargados de la red.

CD's, DVD's, USB's , discos externos o cualquier otro tipo de memoria.

12 Clasificación de los antivirus: [12]

Antivirus preventores: como su nombre lo indica, este tipo de antivirus se caracteriza por anticiparse a la infección, previniéndola. De esta manera, permanecen en la memoria de la computadora, monitoreando ciertas acciones y funciones del sistema.

Antivirus identificadores: esta clase de antivirus tiene la función de identificar determinados programas infecciosos que afectan al sistema. Los virus identificadores también rastrean secuencias de bytes de códigos específicos vinculados con dichos virus.

Antivirus descontaminadores: comparte una serie de características con los identificadores. Sin embargo, su principal diferencia radica en el hecho de que el propósito de esta clase de antivirus es descontaminar un sistema que fue infectado, a través de la eliminación de programas malignos. El objetivo es retornar dicho sistema al estado en que se encontraba antes de ser atacado. Es por ello que debe contar con una exactitud en la detección de los programas

malignos.

Cortafuegos o firewall: estos programas tienen la función de bloquear el acceso a un determinado sistema, actuando como muro defensivo. Tienen bajo su control el tráfico de entrada y salida de una computadora, impidiendo la ejecución de toda actividad dudosa.

Antiespías o antispyware: esta clase de antivirus tiene el objetivo de descubrir y descartar aquellos programas espías que se ubican en la computadora de manera oculta.

Antipop-ups: tiene como finalidad impedir que se ejecuten las ventanas pop-ups o emergentes, es decir a aquellas ventanas que surgen repentinamente sin que el usuario lo haya decidido, mientras navega por Internet.

Antispam: se denomina spam a los mensajes basura, no deseados o que son enviados desde una dirección desconocida por el usuario. Los antispam tienen el objetivo de detectar esta clase de mensajes y eliminarlos de forma automática.

13 Ejemplos de antivirus: [13]

- Avast.
- AVG Antivirus.
- Norton Security.
- McAfee.
- Panda.
- Avira AntiVir Personal.
- Lavasoft.
- Clam.
- Kaspersky.

14 Conclusiones

Los virus pueden ocasionar perdidas de datos, espiarnos o solo molestarnos como lo hacen los que son de tipo gusano. Independientemente si e virus nos moleste o no es un mal que se debe erradicar y para eso las personas deben de proteger sus equipos con un antivirus y un firewall, si todas las personas lo hicieran la propagación de virus se disminuiría pues estos se alojan en equipos contaminados y se van propagando mediante USB o correo. Hay que procurar no navegar por paginas web donde se suelen alojar estos programas y no descargar archivos de estos sitios, así como no abrir los vínculos de correo de dudosa procedencia. Una de las mejores herramientas para prevenir una infección es simplemente el sentido común ya que si visitas una pagina web, por el diseño o características que tenga ese sitio te podrás dar cuenta si debes de confiar en ese sitio o no. Generalmente los virus suelen ocultarse en sitios con menor popularidad o paginas no muy visitadas esperando a que algún internauta caiga en su trampa, que no es nada mas ni nada menos que un simple enlace que te lleva a un lugar que te permita descargar un programa que buscas, pero lo que encuentras no siempre es lo que deseas.

Fuentes:

[1] http://www.pandasecurity.com/mexico/homeusers/security-info/classic-malware/virus/

[2] http://pozarica.ar.tripod.com/Virus.html

[3] http://www2.udec.cl/ sscheel/pagina%
20virus/historia.htm

[4] http://www.pandasecurity.com/mexico/homeusers/security-info/about-malware/technical-data/date-3.htm

[5] http://www.monografias.com/trabajos16/virus-computacionales/virus-computacionales.shtml#histor

[6] http://www.cavsi.com/preguntasrespuestas/que-metodos-utilizan-los-virus-informaticos-para-propagarse/

[7] http://www.seguridad.unam.mx/descarga.dsc?arch=1108

[8] http://soporte.eset-la.com/kb2563/?viewlocale=es_
ES

[9] http://www.seguridadpc.net/evita_
infect.htm

[10] http://www.definicionabc.com/tecnologia/antivirus.php

[11] http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=116

[12] http://www.tiposde.org/informatica/418-tipos-de-antivirus-informaticos/

[13] http://www.ejemplos.org/ejemplos-de-antivirus.html