



TABLA DE CONTENIDO

1. ANTECEDENTES HISTÓRICOS

- 1.1. LOS PRECURSORES. (1939-1949)
- 1.2. 1981 LA IBM PC
- 1.3. 1986 EL COMIENZO DE LA GRAN EPIDEMIA
- 1.4. 1991 LA FIEBRE DE LOS VIRUS
- 1.5. 1991 LOS VIRUS PERUANOS
- 1.6. 1995 LOS MACRO VIRUS
- 1.7. 1999 LOS VIRUS ANEXADOS (adjuntos)
- 1.8. 2000 EN ADELANTE

2. MARCO LEGAL

3. BASES TEÓRICAS DEL TUTORIAL

- 3.1. INTRODUCCIÓN
- 3.2. QUE ES UN VIRUS.
 - 3.2.1. Características de los virus
 - 3.2.2. Daños de los virus
- 3.3. CLASES DE VIRUS
- 3.4. TIPOS DE VIRUS
- 3.5. MÉTODOS DE PROPAGACIÓN DE VIRUS
- 3.6. INTERNET.
- 3.7. INTRUSIÓN POR INTERNET
 - 3.7.1. Daños Causados por los Virus Informáticos





- 3.7.2. Síntomas Típicos de una Infección
- 3.8. QUE SON LOS ANTIVIRUS Y FIREWALL
 - 3.8.1. Antivirus
 - 3.8.1.1. Características del Antivirus
 - 3.8.1.2. Técnica Heurística
 - 3.8.1.3. ¿Cómo opera un antivirus?
 - 3.8.1.4. ¿Cómo valorar un Antivirus?
 - 3.8.2. Firewalls
 - 3.8.2.1. Función de los Firewalls
 - 3.8.2.2. Tipos de Firewalls:
 - 3.8.2.3. Características
- 3.9. MÉTODOS DE PREVENCIÓN
 - 3.9.1. Métodos de Protección
- 3.10. PROCEDIMIENTOS PARA LA DESINFECCIÓN

BIBLIOGRAFÍA





1. ANTECEDENTES HISTÓRICOS

Desde la aparición de los virus informáticos en 1984 y tal como se les concibe hoy en día, han surgido muchos mitos y leyendas acerca de ellos. Esta situación se agravó con el advenimiento y auge de Internet. A continuación, un resumen de la verdadera historia de los virus que infectan los archivos y sistemas de las computadoras¹.

1.1. LOS PRECURSORES. (1939-1949)².

La historia de los virus se remonta desde el año 1939, y comienza básicamente con el famoso científico matemático [John Louis Von Neumann](#), el cual exponía en su teoría la posibilidad de desarrollar programas que pudieran tomar el control de otros.

Luego en 1944 contribuyó en forma directa con [John Mauchly](#) y [J. Presper Eckert](#), en la fabricación de la ENIAC, una de las computadoras de Primera Generación, quienes construyeron además la famosa UNIVAC en 1950.

Esta teoría dio bases a Robert Thomas Morris, Douglas McIlory y Victor Vysotsky, programadores de la Bell Computer a crear un juego al que denominaron CoreWar (1949). El primero de estos tres jóvenes años mas tarde se convierte en padre de [Robert Tappan Morris](#) quien en 1988

¹ <http://www.perantivirus.com/sosvirus/general/histovir.htm>

² Ibid





introdujo un virus en [ArpaNet](#), la precursora de Internet. El juego que había creado su padre en compañía de otros tres chicos ejecutaba programas que iban paulatinamente disminuyendo la memoria del computador y el ganador era el que finalmente conseguía eliminarlos totalmente. Este juego aunque se mantuvo en la clandestinidad, fue motivo de concursos en importantes centros de investigación como el de la Xerox en California y el Massachusetts Technology Institute (MIT), entre otros.

También existen reportes acerca del virus Creeper, creado en 1972 por Robert Thomas Morris, que atacaba a las famosas 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 del software antivirus.

1.2. 1981 LA IBM PC³.

En Agosto de 1981 la International Business Machine lanza al mercado su primera computadora personal, simplemente llamada IBM PC. 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

³ Ibid





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.

Sin embargo fue en 1984, y a causa de Fred Cohen, quien publicó un libro de cómo desarrollar virus, cuando los usuarios del BIX BBS, un foro de debates de la ahora revista BYTE reportaron la presencia y propagación de algunos programas que habían ingresado a sus computadoras en forma subrepticia, actuando como "caballos de troya", logrando infectar a otros programas y hasta el propio sistema operativo, principalmente al Sector de Arranque. 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.

1.3. 1986 EL COMIENZO DE LA GRAN EPIDEMIA⁴.

En 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 diskettes. Posteriormente aparecieron los virus que infectaban los archivos con extensión EXE y COM.

⁴ Ibid





El 2 de Noviembre de 1988 Robert Tappan Morris, difundió un virus a través de ArpaNet, (precursora de Internet) logrando infectar 6,000 servidores conectados a la red. La propagación la realizó desde uno de los terminales del MIT (Instituto Tecnológico de Massachussets). Quien al ser descubierto, fue enjuiciado y condenado en la corte de Syracuse, estado de Nueva York, a 4 años de prisión y el pago de US \$ 10,000 de multa, pena que fue conmutada a libertad bajo palabra y condenado a cumplir 400 horas de trabajo comunitario. Actualmente es un experto en Seguridad y ha escrito innumerables obras sobre el tema.

1.4. 1991 LA FIEBRE DE LOS VIRUS⁵.

En 1989 el virus Dark Avenger o el "vengador de la oscuridad", se propagó por toda Europa y los Estados Unidos haciéndose terriblemente famoso por su ingeniosa programación, peligrosa y rápida técnica de infección. En el año de 1992, los búlgaros después de reconocer el liderazgo de su país en la mutación de virus, se cansaron y empezaron a desarrollar sus propias creaciones.

⁵ Ibid





1.5. 1991 LOS VIRUS PERUANOS⁶.

Al igual que la corriente búlgara, en 1991 apareció en el Perú el primer virus local, autodenominado Mensaje y que era una simple mutación del virus Jerusalem-B y al que su autor le agregó una ventana con su nombre y número telefónico. Los virus con apellidos como Espejo, Martínez y Aguilar fueron variantes del Jerusalem-B y prácticamente se difundieron a nivel nacional. En 1993 empezaron a crearse y diseminarse especies nacionales desarrolladas con creatividad propia, como los virus Katia, Rogue o F03241 y los polimórficos Rogue II y Please Wait (que formateaba el disco duro).

1.6. 1995 LOS MACRO VIRUS⁷.

A mediados de 1995 apareció en diversas ciudades del mundo 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. En 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.

⁶ Ibid

⁷ Ibid





1.7. 1999 LOS VIRUS ANEXADOS (adjuntos)⁸.

A 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 [Melissa](#). Ese mismo año fue difundido a través de Internet el peligroso [CIH](#) y el [ExploreZip](#), entre otros muchos más. A fines de Noviembre de este mismo año apareció el [BubbleBoy](#), primer virus que infecta los sistemas con tan sólo leer el mensaje de correo, el mismo que se muestra en formato HTML. En Junio del 2000 se reportó el [VBS/Stages.SHS](#), primer virus oculto dentro del Shell de la extensión .SHS.

1.8. 2000 EN ADELANTE⁹.

Los verdaderos codificadores de virus, no los que simplemente los modifican, han re-estructurado sus técnicas y empezado a demostrar una enorme malévolas creatividad. El 18 de Septiembre del 2001 el virus [Nimda](#) amenazó a millones de computadoras y servidores, a pocos días del fatídico ataque a las Torres Gemelas de la isla de Manhattan, demostrando no solo la vulnerabilidad de los sistemas, sino la falta de previsión de muchos de los administradores de redes y de los usuarios.

⁸ Ibid

⁹ Ibid





Los gusanos, troyanos o la combinación de ellos, de origen alemán como [MyDoom](#), [Netsky](#), etc. revolucionaron con su variada técnica.

No se puede dejar de mencionar la famosa "[Ingeniería Social](#)", culpable de que millones de personas caigan en trampas, muchas veces ingenuas. Los [BOT de IRC](#) y a finales del 2005 los temibles [Rootkit](#). Resultará imposible impedir que se sigan desarrollando virus en todo el mundo, por ser esencialmente una expresión cultural de "graffiti cibernético", así como los crackers jamás se detendrán en su intento de "romper" los sistemas de seguridad de las redes e irrumpir en ellas con diversas intencionalidades. Podemos afirmar que la eterna lucha entre el bien y el mal ahora se ha extendido al ciber espacio.





2. MARCO LEGAL

La legislación colombiana ofrece muy pocas opciones de penalización a los delitos informáticos, dentro del Código Penal no se hace referencia suficiente al tema de delitos informáticos comparado con países como España Alemana que si los consagran de manera más explícita y organizada.

Los delitos informáticos en Colombia están encuadrados dentro de los delitos tradicionales. Lo que más se asemeja al tema de los delitos informáticos está únicamente en los artículos 192, 193 y 195 del Código Penal, pero estos no están plenamente diseñados para este tipo de conductas

- El artículo 192 trata sobre la Violación ilícita de comunicaciones
- El Artículo 193 trata sobre el Ofrecimiento, venta o compra de un instrumento apto para interceptar la comunicación privada entre personas.
- El artículo 195 trata sobre el Acceso abusivo a un sistema informático.

Las penas impuestas a los delincuentes informáticos son:

- La violación ilícita de comunicación o correspondencia oficial con 3 a 6 años de cárcel.





- La utilización ilícita de equipos transmisores o receptores (WiFi) se penaliza con 1 a 3 años
- La violación ilícita de comunicaciones con 2 a 4 años en el peor escenario
- Delito de sabotaje con uno a seis años y multa de 5 a 20 salarios mínimos.

Cabe destacar que las penas en nuestro país son muy bajas comparadas con otros países.



3. BASES TEÓRICAS DEL TUTORIAL

3.1. INTRODUCCIÓN

Los virus, gusanos y troyanos son programas malintencionados que pueden provocar daños en el equipo y en la información del mismo. También pueden hacer más lento Internet e, incluso, pueden utilizar su equipo para difundirse a amigos, familiares, colaboradores y el resto de la Web. La buena noticia es que con un poco de prevención y algo de sentido común, es menos probable ser víctima de estas amenazas.

3.2. QUE 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. Se dice que es un programa parásito porque el programa ataca a los archivos o sectores de "boot" 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.

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.

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 (Secreto, escondido, encubierto)

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 subrepticamente. 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.

3.2.1. 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. Para alcanzar su objetivo de filtrarse y contagiar, cumplen con características como:





- **Encriptamiento:** el virus se encripta en [símbolos](#) sin sentido para no ser detectado, pero para destruir o replicarse DEBE descryptarse 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 tecléo; un macro o la apertura de un programa asociado al virus (Troyanos).

3.2.2. 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 sobre escribe 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.

3.3. CLASES DE VIRUS

-  **Camaleones:** Son una variedad de virus similares a los Caballo de Troya que actúan como otros programas parecidos, en los que el usuario confía, mientras que en realidad están haciendo algún tipo de daño. Bien programados, pueden realizar todas las funciones de los programas legítimos a los que sustituyen. Un software camaleón podría, por ejemplo, emular un programa de acceso a sistemas remotos realizando todas las acciones que ellos realizan; pero como tarea adicional y oculta a los usuarios, va almacenando en algún archivo los diferentes logins y passwords para que posteriormente puedan ser recuperados y utilizados ilegalmente por el creador del virus.
- **Bombas:** Pueden ser de tres tipos:





- **Bombas de software.** Durante tiempo fueron el código más fácil de programar y reproducir detonan a los pocos segundos de ser ejecutadas sin avisar al usuario y producen, generalmente, una pérdida total de los datos del computador en general no se reproducen.
- **Bombas lógicas.** Parecidas a las anteriores, realizan algún tipo de acción destructiva dependiendo del estado de algunas variables de ambiente del sistema donde actúan. Por ejemplo, podría esperar que su creador ingrese periódicamente una contraseña y empezar a actuar cuando la misma no es provista por un tiempo determinado produciendo la destrucción de los datos del sistema.
- **Bombas de tiempo.** Son técnicamente iguales a las lógicas, ya que actúan condicionadas a alguna variable del ambiente relacionada con el tiempo.
- **Reproductores.** Se reproducen en forma constante una vez que son ejecutados hasta agotar totalmente el espacio de disco o memoria del sistema. La única función de este virus es crear clones y lanzarlos a ejecutar para que ellos hagan lo mismo. Su finalidad es agotar los recursos del sistema, hasta que el sistema principal no puede continuar con el procesamiento normal.
- **Gusanos.** Son programas que constantemente viajan a través de un sistema informático





interconectado sin dañar necesariamente el hardware o el software de los sistemas que visitan. La función principal es viajar en secreto a través de equipos anfitriones recopilando cierto tipo de información programada para enviarla a un equipo determinado al cual el creador del virus tiene acceso.

- **Caballos De Troya:** Del mismo modo que el caballo de Troya mitológico, los troyanos de hoy en día son programas informáticos que parecen ser software útil pero que ponen en peligro la seguridad y provocan muchos daños. Por tal razón se conocen como aquellos virus que se introducen en el sistema bajo una apariencia totalmente diferente a la de su objeto final, esto es, que se presentan como información perdida sin ningún sentido. Al cabo del tiempo, esperando a la indicación programada, se activan, comienzan a ejecutarse y a mostrar sus verdaderas intenciones. Estos virus son destructores de la información contenida en los discos.
- **Virus De Macro:** Macro es un conjunto de instrucciones para ser llevadas a cabo por un programa de computador. Estas instrucciones se emplean típicamente para hacer tareas.- Un virus de macro es una macro, el cual se enmascara como un legítimo archivo, generalmente de Microsoft Word. Este virus utiliza la macro para replicarse y realizar algún tipo de daño. Las instrucciones que contiene este virus de macro pueden copiar y borrar archivos, realizar modificaciones a los archivos, insertar





otros virus y ejecutar programas incluyendo el virus que ha insertado. No son directamente ejecutables, sino que deben ser leídos, interpretados y ejecutados. Hoy en día los virus de macro son los más peligrosos y extendidos.- Por encontrarse muy extendidos a causa de Internet los convierte en la mayor amenaza contra la seguridad informática del mundo.

3.4. 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.

3.5. MÉTODOS DE PROPAGACIÓN DE VIRUS

La manera más común de transmitir un virus es inicializando un ordenador con un disquete infectado en el drive A. El disquete infectado automáticamente escribe su código en el sector de arranque maestro.





Este sector se ejecuta cada vez que se inicia el ordenador, por lo que el virus se ejecuta cada vez que se inicia el ordenador. El sector de arranque maestro se ejecuta independientemente del sistema operativo que esté utilizando (DOS, Windows 95, OS/2, Windows NT, UNIX, etc.,). Una vez que el virus ha infectado el ordenador, éste tiene dos misiones principales: propagarse a sí mismo y activar su "gatillo" (el evento que provoca al virus desarrollar su tarea). Para propagarse a sí mismo, el virus necesita encontrar un "portador". Un "portador" puede ser un fichero u otro disquete. La mayoría de sectores de arranque propagan el virus a cada nuevo disquete introducido en la disquetera. Si el portador es un fichero, y este fichero se ejecuta en el sistema de otro usuario, el sector de arranque quedará infectado por el virus.

De igual manera se puede ser víctima de una infección al:

- Realizar una descarga o ejecución de ficheros adjuntos a correos electrónicos.
- Visitar ciertos tipos de páginas web que utilizan un componente llamado ActiveX o Java Applet.
- Leyendo un e-mail dentro de ciertos tipos de programas de e-mail como Outlook o Outlook Express.

3.6. INTERNET.

Internet es un método de interconexión de computadoras implementado en un paquete de protocolos denominado TCP/IP, y garantiza que redes





físicas heterogéneas funcionen como una red (lógica) única. De ahí que Internet se conozca comúnmente con el nombre de "red de redes", pero es importante destacar que Internet no es un nuevo tipo de red física, sino un método de interconexión. Aparece por primera vez en 1969, cuando ARPAnet establece su primera conexión entre tres universidades en California y una en Utah. También se usa el término Internet como sustantivo común y por tanto en minúsculas para designar a cualquier red de redes que use las mismas tecnologías que Internet, independientemente de su extensión o de que sea pública o privada.

Al contrario de lo que se piensa comúnmente, Internet no es sinónimo de World Wide Web (WWW). Ésta es parte de Internet, siendo la World Wide Web uno de los muchos servicios ofertados en la red Internet. La Web es un sistema de información mucho más reciente, desarrollado inicialmente por Tim Berners Lee en 1989. El WWW utiliza el Internet como medio de transmisión.

Algunos de los servicios disponibles en Internet aparte de la Web son:

- El acceso remoto a otras máquinas (SSH y telnet),
- Transferencia de archivos (FTP),
- Correo electrónico (SMTP),
- Boletines electrónicos (news o grupos de noticias),
- Conversaciones en línea (IRC y chats),
- [Mensajería instantánea](#),
- Transmisión de archivos (P2P, P2M, Descarga Directa), etc.





3.7. INTRUSIÓN POR INTERNET

La existencia y el uso masivo del Internet le han dado una dimensión más amplia a la intrusión de virus informáticos a los ordenadores, e incluso a las redes.

Años atrás, los virus informáticos se difundían a través de soportes físicos como los discos flexibles en la mayoría de casos por lo tanto, su difusión era mucho más lenta. La mayoría de los daños causados por virus a través de Internet vienen de virus conocidos que explotan nuevos métodos de transmisión. Existen dos formas básicas de difusión: la distribución accidental y la maliciosa.

- **Distribución inocente de virus:** Compartir y descargar software a través de Internet es especialmente fácil. Un simple clic de ratón añade un documento a un correo o permite descargar un nuevo programa. Si ese documento o programas están infectados el receptor infectará su sistema al ejecutarlos. Los virus más difundidos a través de Internet son los virus de macro. Están anexionados a datos, no a código, y eso hace mucho más difícil su detección. Nunca debe abrir documento alguno sin testarlo previamente.
- **Distribución maliciosa de virus:** Algunos programadores de virus utilizan Internet como una vía rápida para la difusión de sus virus. Los presentan como ficheros atractivos con objeto de que el





mayor número posible de usuarios los descarguen y se contagien. La precaución es su mejor arma en este caso. No descargue programas si no está completamente seguro y confía en la fuente. No abra los documentos con la aplicación que fueron creados, utilice un visor.

3.7.1. Daños Causados por los Virus Informáticos. Algunos ejemplos de daños causados por virus pueden ser:

- Pérdida de datos.
- Corrupción de los datos del disco duro
- Modificación de los datos de documentos o hojas de cálculo añadiendo datos o corrompiendo los originales del documento
- Pérdida de confidencialidad.





3.7.2. Síntomas Típicos de una Infección. Nunca se está exento de la posibilidad de que su ordenador sufra una infección por estos virus. Esto es debido a la cada vez mayor profusión y creación de este tipo de engendros informáticos, unido a la mayor utilización de los recursos e información disponibles en Internet y del correo electrónico. Por lo tanto se deben conocer los "síntomas" de estas infecciones.

Algunos de los síntomas que pueden presentar un equipo o sistema infectado son los siguientes:

- 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](#) continúa parpadeando aunque no se esté 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 está advertido).
- Los caracteres de texto se caen literalmente a la parte inferior de la pantalla (especialmente en DOS).
- En la pantalla del [monitor](#) pueden aparecer 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...!!).

Otros de los síntomas que se presentan en ordenadores son:

En directorios y archivos:

- La cantidad de espacio disponible es cada vez menor.
- Aumento de longitud (bytes) de los archivos
- Algunos archivos desaparecen del disco (borrados).
- El directorio muestra archivos desconocidos por el usuario.
- Los archivos son sustituidos por caracteres ilegibles.
- Alteración en la indicación de la hora de un archivo.

En la ejecución de aplicaciones

- Los programas tardan más tiempo en cargarse o no son operativos.





- Algunas aplicaciones trabajan más lentamente que lo normal.
- Al abrir un archivo aparecen errores que antes no existían.
- Al solicitar la apertura de un archivo aparecen en el menú drivers que no están instalados.

Funcionamiento del sistema:

- Rendimiento del sistema reducido.
- La cantidad de memoria disponible cambia o disminuye continuamente.
- Arranque incompleto del sistema o fallo en el arranque.
- Escrituras inesperadas en una unidad.
- Mensajes de error extraños o no estándar.
- Actividad de pantalla no estándar (animaciones, etc.), fluctuaciones de pantalla.
- Sectores erróneos en disquetes y en discos duros.
- Cualquier operación extraña que su ordenador no realizaba antes y que de un momento a otro comienza a ejecutar.
- Errores no justificados en la FAT.
- Síntomas de macrovirus en Word
- Los documentos de Word solo pueden ser guardados como plantillas.
- Los archivos eliminados no son recuperables.
- Los archivos muestran un cuadro de dialogo con un número 1.
- Nuevas macros, llamadas AAAZAQ, AAAZFS y PayLoad, aparecen en la lista de macros de Word.





- El archivo Winword.ini contiene la línea ww6=1
- Alteraciones en el archivo Normal.dot a partir de la comparación de esta plantilla con una copia anterior, previamente guardada en una carpeta del disco, utilizando comandos como el FC.EXE o el diff desde el AUTOEXEC.BAT.
- Alteraciones en la carpeta de INICIO (STARTUP) de Microsoft Word, que pueden ser debidas a la inclusión de nuevas plantillas o de alteraciones en las plantillas allí contenidas.

3.8. QUE SON LOS ANTIVIRUS Y FIREWALL

3.8.1. Antivirus. Programa creado para prevenir o evitar la activación de los virus, así como su propagación y contagio. Cuenta además con rutinas de detención, eliminación y reconstrucción de los archivos y las áreas infectadas del sistema.

3.8.1.1. Características del Antivirus. Un antivirus tiene tres principales funciones y componentes:

- **Vacuna** es un programa que instalado residente en la memoria, actúa como "filtro" de los programas que son ejecutados, abiertos para ser leídos o copiados, en tiempo real. Una vacuna al instalarse queda residente en memoria, de esta manera avisa de diversos sucesos. Por ejemplo, cuando un programa ha solicitado quedarse residente en memoria, que está intentando modificar alguno de los archivos del sistema o algún archivo ejecutable o se





pretende hacer alguna operación de borrado general. Dos de las vacunas más comunes en PC´s son: Vshield y Vsafe.

- **Detector**, que es el programa que examina todos los archivos existentes en el disco o a los que se les indique en una determinada ruta o PATH. Tiene instrucciones de control y reconocimiento exacto de los códigos virales que permiten capturar sus pares, debidamente registrados y en forma sumamente rápida desarmar su estructura.
- **Eliminador** es el programa que una vez desactivada la estructura del virus procede a eliminarlo e inmediatamente después a reparar o reconstruir los archivos y áreas afectadas.

3.8.1.2. Técnica Heurística. Entiéndase como indicador de probabilidad de contagio, esto nos lleva a considerarla como un sistema de detección mejorada que al incluirla los antivirus nos permite establecer un sistema de alerta y de prevención ante la aparición de mutaciones de virus o de nuevos virus.

Surge de la necesidad de una "detección genérica" de los virus informáticos. Se llama detección genérica a la posibilidad de detectar "cualquier virus" aún sin haberlo analizado antes y sin estar en la base de datos del antivirus que se esté considerando. Esto pareciera que carece de sentido pero es tan simple como buscar "instrucciones





comunes” de los virus para advertir de la posibilidad de que un archivo o programa esté infectado.

El funcionamiento de la heurística es sencillo, primero se analiza cada programa sospechoso sin ejecutar las instrucciones, lo que hace es desensamblar o "descompilar" el código de máquina para deducir que haría el programa si se ejecutara. Avisando que el programa tiene instrucciones para hacer algo que es raro en un programa normal, pero que es común en un virus.

3.8.1.3. ¿Cómo opera un antivirus? Los virus tienen patrones de códigos que son como sus "huellas digitales". Los software antivirus buscan estos patrones, pero sólo de los que tienen almacenados en su lista (por esto la actualización es tan importante). Estos productos también pueden valerse de la heurística, es decir, analizan los archivos para detectar comportamientos similares a los de los virus.

Cada día crece el número de nuevos virus y la alternativa para poder neutralizarlos, sin haber programado antes el antivirus para su reconocimiento, es la denominada "búsqueda heurística". A través de ella, el programa antivirus analiza el código de los programas buscando instrucciones, acciones sospechosas o indicios que delaten la presencia de virus en la computadora, de acuerdo a los patrones habituales empleados por los códigos maliciosos.





3.8.1.4. ¿Cómo valorar un Antivirus? Los factores más importantes a la hora de valorar un antivirus son:

- **Capacidad de detección y desinfección**
- **Heurística**
- **Velocidad:** Hoy en día los discos duros son enormes, y si pensamos en intranets y redes corporativas la cantidad de datos a escanear puede ser colosal. Por lo tanto se valorará en un antivirus la capacidad de escanear rápidamente.
- **Actualización**

RECOMENDACIÓN: HAY ALGO QUE QUIZÁ SEA UN CONSEJO FUNDAMENTAL. NO SE PUEDE CONFIAR PLENAMENTE EN UN ANTIVIRUS. Cada uno tiene sus limitaciones y trabas, por lo tanto, la mejor forma de evitar una infección es la prevención.

3.8.2. Firewalls. (A prueba de fuego). Conjunto de programas de protección y dispositivos especiales que colocan barreras al acceso exterior a una determinada red privada. Es utilizado para proteger los recursos de una organización, de consultas externas no autorizadas.

Dado lo peligrosamente vulnerables que se han vuelto actualmente las redes es necesario contar con alguna barrera que controle el flujo de información y evite así la entrada de intrusos al sistema, esta es la tarea de la cual se encargan los firewalls los cuales son una importante herramienta de seguridad en la actualidad.





3.8.2.1. Función de los Firewalls. Tienen como principal función:

- Impedir accesos a usuarios no autorizados (no importa si viene de red local o Internet)
- Bloquear algunos programas troyanos y otras aplicaciones capaces de dañar el sistema
- Examinar el contenido de la información que se está obteniendo para determinar si se le permite el paso a nuestra computadora o no (filtrado).
- Las políticas de control de los datos que ocupa varían de acuerdo al firewall que se utilice.

3.8.2.2. Tipos de Firewalls:

- Aquellos que Filtran los datos en base a sus contenidos y dirección IP
- Aquellos que Solo permiten la comunicación entre computadoras admitidas y proveedores de servicio de Internet
- Aquellos Que realiza una inspección de estado controlando la configuración de los paquetes para decir si son útiles o no y luego decide si bloquea o no el paso de la información. Para que un firewall sea efectivo, todo trafico de información a través de Internet deberá pasar a través del mismo para ser inspeccionado.





3.8.2.3. Características. Los firewalls reciben información y deciden si esta pasa o no, pero la información ya se recibió. Un buen ejemplo del funcionamiento del firewall es aquel que compara el puerto que protege el firewall con un tubo, El firewall tapa uno de los extremos del tubo, luego analiza la información, si la información cumple con los requisitos impuestos por el firewall, pasa a las aplicaciones del computador sino llega hasta ahí no más.

Cuando los paquetes llegan al computador, van al OTRO extremo del tubo - el extremo TCP/IP. Si el propósito del paquete es dañar el extremo que lo recibe, es inútil cerrar el puerto hacia la aplicación. Más aun, es imposible protegerse contra todos los tipos de ataque, lo que demuestra que no es 100% efectivo. Entonces podemos considerar a los firewalls como un buen sistema de seguridad, pero no debe dejarse todo en sus manos, sino que debe implementarse con Antivirus.





3.9. MÉTODOS DE PREVENCIÓN

Consejos para proteger tu PC.

- Utiliza un buen antivirus y actualízalo frecuentemente.
- Comprueba que tu antivirus incluye soporte técnico
- Asegúrate de que tu antivirus esté siempre activo.
- Verifica, antes de abrir, cada nuevo mensaje de correo electrónico recibido
- Evita la descarga de programas de lugares no seguros en Internet.
- Rechaza archivos que no hayas solicitado cuando estés en chats o grupos de noticias (news).
- Actualiza el software que tienes instalado con los parches aconsejados por el fabricante de este programa.
- Retira los disquetes de las disqueteras al apagar o reiniciar tu ordenador.
- Analiza el contenido de los archivos comprimidos.
- Mantente alerta ante acciones sospechosas de posibles virus.
- Añade las opciones de seguridad de las aplicaciones que usas normalmente a tu política de protección antivirus.
- Realice periódicamente copias de seguridad.
- Mantente informado.
- Utiliza siempre software legal.





3.9.1. Métodos de Protección. Los métodos para contener o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos.

- **Activos.**

- **Antivirus:** los llamados programas [antivirus](#) tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.
- **Filtros de ficheros:** consiste en generar filtros de ficheros dañinos si el ordenador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de [correos](#) o usando técnicas de [firewall](#). En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.

- **Pasivos.**

- **Copias de seguridad:** Mantener una política de [copias de seguridad](#) garantiza la recuperación de los datos y una solución cuando nada de lo anterior ha funcionado.





- **Estudiar:** Aprender como es el software de nuestra computadora, buscando y buscando información, en sitios en los que se pueda confiar, sobre software dañino, para así evitarlo.
- **Desconfiar:** Si no conocemos algo o no sabemos lo que hace, será mejor tenerle respeto y no tocarlo hasta aclarar nuestra duda, (en el uso de esta regla es recomendable no abrir archivos de correos de los que se desconoce el remitente, o se sospecha de que pueda contener código malicioso, o que no pidió usted. Aun así, si es de entera confianza, analice siempre con un antivirus el archivo antes de abrirlo).
- **Hacer reenvíos seguros de email:** cuando recibamos un mensaje de correo electrónico sospechoso de contener virus o que hable de algo que desconocemos conviene consultar su posible infección o veracidad (por ejemplo a partir de buscadores de la www). Sólo si estamos seguros de la ausencia de virus del mensaje o de que lo que dice es cierto e importante de ser conocido por nuestros contactos lo reenviaremos, teniendo cuidado de poner las direcciones de correo electrónico de los destinatarios en la casilla [CCO](#).
- **Informar a nuestros contactos:** Conviene que hagamos saber lo mencionado en el punto anterior a nuestros contactos en cuanto nos reenvían mensajes con virus o contenido falso o sin utilizar la casilla CCO.

3.10. PROCEDIMIENTOS PARA LA DESINFECCIÓN





Es conveniente mencionar que dependiendo del caso y el nivel de conocimientos del sistema que se tenga individualmente, así será la solución a seguir. Por tal caso, se mencionaran a continuación varias formas típicas de proceder ante una infección de virus informático en su PC.

- **Limpiar y eliminar el virus:** En el caso de que nuestra máquina resulte infectada debemos proceder a su desconexión inmediata de la red, ya sea local o Internet (esto se hace para evitar contagios a otras máquinas) y, una vez aislada, aplicar un programa Antivirus actualizado para tomar la acción que se corresponda.
- **Restauración completa:** En caso de que el virus sea tan virulento que destruya la lógica de una unidad de almacenamiento, se deberá recurrir a la restauración completa con formateo completo. Téngase en cuenta que esta operación dejará la máquina tal y como estaba el día que se adquirió. Sus configuraciones y demás quedarán borradas permanentemente, es por esta razón la importancia de realizar Backups constantemente, ya que en este caso se podrá salvar parte de la información.





BIBLIOGRAFÍA

BORUELO Cristian Fabián. Seguridad informática sus implicancias e implementación. Sep. del 2001. 203 págs.

CLOUGH Bryan y MUNGO Paul, Los piratas del chip. Ediciones B.

Enciclopedia Océano, Tomo IV; Cap. "El mundo de las Computadoras".

HERNÁNDEZ, Roberto. Firewalls: Seguridad en las redes e Internet Boletín de Política Informática N° 2. Página 7. España. 2000.

JACOBSON, BOOCH, RUMBAUGH. El proceso unificado de desarrollo de software. Pearson Educación Madrid 2000. 464 páginas.

MONSERRAT Coll Francisco. Seguridad en los protocolos. Página 30.

SENA Mayans Leonardo. Seguridad Informática. Julio 2000, 11paginas.

Rey Jiménez, Alexandra y Leal aponte, Marcela. Lenguaje Unificado de Modelamiento (UML) [en línea]. Citado el 13 de Abril del 2007.

Disponible en Internet en: <http://www.creangel.com/uml/intro.php>

Introducción a ASP [en línea]. Citado el 14 de Marzo 2007. Disponible en Internet en: <http://www.aspespañol.com/tutorial/ASP.htm>.





Leyva, Juan. Uml - Página personal de Juan Leyva - Artículos, tutoriales, proyectos y aplicaciones desarrolladas por Juan Leyva [en línea]. Citado el 14 de Abril del 2007. Disponible en Internet en: <http://juanleyva.metricasweb.com/tutoriales/uml>

Borguello, Cristian. Concepto de virus troyanos. Citado el 20 de octubre del 2006. Disponible en internet en: <http://www.segu-info.com.ar/malware/troyano.htm>

Borguello, Cristian. Seguridad informática-creación y difusión de virus. Citado el 20 de octubre del 2006. Disponible en internet en: <http://www.segu-info.com.ar/virus/virus.htm>

Álvarez Marañón, Gonzalo. Hablan los expertos- Virus. Citado el 25 de octubre 2006. Disponible en internet en: <http://www.iec.csic.es/CRIPTONOMICON/articulos/virus.html>

Machado, Jorge. Historia de los virus informáticos. Citado el 1 de mayo del 2007. Disponible en internet en: <http://www.perantivirus.com/sosvirus/general/histovir.htm>

Historia de la Computación. Citado el 1 de mayo del 2007. Disponible en internet en: <http://etsiit.ugr.es/alumnos/mlii/univac.htm>

Wikipedia. Concepto de Cracker y Hacker. Citado el 20 de febrero del 2007. Disponible en internet en: <http://es.wikipedia.org/wiki/Cracker>





Seguridad PC. Como prevenir los virus. Citado el 4 de mayo del 2007.
Disponible en internet en: http://www.seguridadpc.net/evita_infect.htm

Antivirus.cc. Todo sobre virus y Antivirus. Citado el 5 de mayo del 2007.
Disponible en internet en:
http://www.publispain.com/antivirus/que_son_los_virus.html

Manson, Marcelo. Estudio sobre los Virus informáticos y Antivirus. Citado el 15 de noviembre del 2006. Disponible en internet en:
<http://www.monografias.com/trabajos/estudiovirus>

Microsoft. Que son virus gusanos, troyanos y como prevenirlos. Citado el 29 de abril del 2007. Disponible en internet en:
<http://www.microsoft.com/latam/athome/security/viruses/virus101.msp>
x#EPC

El País. Animación sobre las bases teóricas de los virus informáticos.
Citado el 15 de mayo del 2007. Disponible en internet en:
http://www.elpais.com/fotogalerias/popup_animacion.html?xref=20030129elpepnet_1 bases teóricas del antivirus

La Vanguardia. Animación Flash de cómo se propagan los virus. Citado el 10 de mayo del 2007. Disponible en internet en:
<http://www.lavanguardia.es/multimedia/sen/temasafondo/virusflash.swf>





como se propagan los virus.

AltoSpam. Programa antispam y antivirus – Animación acerca del funcionamiento de los Firewall. Citado el 15 de mayo del 2007.

Disponible en internet en:

<http://www.altospam.com/es/animacion-flash.php> como funcionan los firewall.

Panda Software. Animación acerca del funcionamiento de los antivirus. Citado el 16 de mayo del 2007. Disponible en internet en:

http://www.pandasoftware.es/virus_info/flash/truprevent_tec.swf?NRMODE=Published&NRORIGINALURL=%2fabout%2fprensa%2fTruPrevent_tec.swf&NRNODEGUID=%7b94211412-504B-42F3-B635-55960EEBD124%7d&NRCACHEHINT=NoModifyGuest

Mcafee. Animación del antivirus Mcafee, Donde muestra el mundo dentro de la computadora y a este amigo mecafee cuando llega un correo no deseado. Citado el 16 de mayo del 2007. Disponible en internet en:

<http://losfilosofos.blogspot.com/search/label/Animaciones>

