UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

“LA CULTURA DE LA SEGURIDAD INFORMÁTICA BASADA EN LA PROTECCIÓN ANTE CUALQUIER TIPO DE VIRUS INFORMÁTICO O SOFTWARE MALICIOSO”

T E S I S

PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A

ANGEL GEOVANNI VALLE ARELLANO

ASESOR: ING. JOSÉ ANTONIO ÁVILA GARCÍA

MÉXICO 2012

AGRADECIMIENTOS

Quiero agradecer a la Universidad, a mis profesores, a mi asesor y a todas aquellas personas que me brindaron sus conocimientos para poder lograr una meta importante en mi vida.

A mis abuelitos por su gran y enorme cariño, a mi abuelito por su alentador y maravilloso apoyo, a mi abuelita que desde el cielo nunca me abandonó, a mis padres por su valioso esfuerzo y sacrificio, al amor de mi vida por su incondicional, bello y hermoso amor.

Unas cuantas líneas, no describen el inmenso y enorme agradecimiento que les tengo por haber creído en mí, gracias por hacer que uno de mis sueños se haya convertido en realidad.

ÍNDICE

II ANTIVIRUS

III SEGURIDAD, MÉTODOS DE PROTECCIÓN Y SISTEMA OPERATIVO

IV FORMACIÓN DEL USUARIO PARA LA PREVENCIÓN DE POSIBLES ATAQUES INFORMÁTICOS Y SÍNTOMAS DE CONTAGIO DE VIRUS

V ACCIONES Y PLAN DE CONTINGENCIA PARA ATAQUES INFORMÁTICOS

INTRODUCCIÓN

En la actualidad no existe empresa de informática en el mundo que pueda avalar el cien por ciento de seguridad ante un eventual ataque de los virus, ya que estos evolucionan minuto a minuto.

La seguridad informática se encarga de salvaguardar nuestra información, que es el resultado de procesar los datos. La cual se almacena y se procesa en computadores, que pueden ser independientes o estar conectados a sistemas de redes, esta misma se encuentra expuesta a ciertos riesgos como lo puede ser que se exponga para fines poco éticos, puede divulgarse sin autorización de su propietario o puede estar sujeta a robos, sabotaje y fraudes por resumir, puede ser alterada, destruida y mal utilizada.

La Seguridad Informática también conocida como **S.I.** es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos. La responsabilidad de aplicarlos recae en cada usuario.

Para lograr sus objetivos, la seguridad informática se fundamenta en tres principios que debe cumplir todo sistema informático los cuales son: Confidencialidad, Integridad y Disponibilidad.

La Confidencialidad se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático. Las herramientas de seguridad informática deben proteger el sistema de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

La Integridad alude a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático. Las herramientas de

seguridad informática deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es particularmente importante en sistemas descentralizado, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

La Disponibilidad menciona la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran. Este último principio es particularmente cuyo compromiso con el usuario es prestar servicio permanente.

Esta investigación tiene como finalidad analizar el gran crecimiento del sector de la seguridad informática basada en la temática del virus y los antivirus, así como los diferentes tipos de malwares que existen en la actualidad y el proceso de funcionamiento de los antivirus para su correcta operación.

Al igual que en la medicina, es mejor prevenir que curar los posibles daños que puedan afectar el buen funcionamiento del sistema, existen diversos factores por los cuales se toma la decisión de optar por algún software antivirus, entre los cuales se incluye el costo, desempeño funcionalidad, alcance, entre otras.

Los Objetivos Generales son conocer un panorama amplio acerca de los antivirus y a su vez, entender que tan importantes son para la informática de hoy en día, ofrecer claros ejemplos de cómo la seguridad informática es cada vez más relevante con el paso de los días, esto a cualquier nivel que se le presente, ya sea a personal, empresarial o mundial.

Observar las Ventajas y Desventajas de los diversos Softwares Antivirus, con la finalidad de salvaguardar toda la información digital.

Analizar, el gran impacto que con lleva la falta de protección respecto a los softwares maliciosos.

Adquirir los conocimientos computacionales para la prevención y eliminación de posibles amenazas informáticas.

Mostrar las ventajas que con lleva tener una buena noción de la protección del sistema de cómputo, así como las medidas de planeación que se deben tomar en cuenta en caso de alguna amenaza de cualquier tipo de virus informático.

Los Objetivos Específicos son generar acciones preventivas para la obtención de buenas prácticas de seguridad y protección contra los virus informáticos y desarrollar un plan de contingencia para reducir al máximo las posibles acciones que se puedan presentar ante cualquier tipo de riesgo al sistema operativo.

Con lo cual surge La Hipótesis de saber si realmente existe algún antivirus capaz de ser cien por ciento confiable, eficiente y no vulnerable frente a las diversas amenazas que hoy en día existen en el mundo informático

En el primer capítulo se explica la historia de la computadora, su estructuramiento, funcionamiento y evolución, se da a conocer el significado de lo que es un virus informático, su clasificación, sus características, sus métodos de propagación, entre otras.

En el segundo capítulo se define el significado de Antivirus, el funcionamiento del mismo, así como también recalcando los diferentes tipos de complementos que pueden llegar a tener los antivirus y de tal manera que se puedan comparar las ventajas y desventajas de diferentes softwares antivirus para así poder elegir el que aporte mayores beneficios.

En el capítulo tres se abordan los diversos métodos de protección que podemos tener en contra de los virus informáticos o softwares maliciosos. Se mencionan también las medidas de seguridad a las que como usuarios se recurren para salvaguardar información en caso de que el equipo de cómputo se encuentre infectado por algún virus. Se explica a detalle el significado de una plataforma informática ya que es de suma importancia comprender este término para poder comprender la magnitud de los ataques de los virus. Conocer a detalle que es el

sistema operativo, cómo trabaja, que finalidad tienen y así tener un mayor conocimiento de las diferentes plataformas que hoy en día existen en el ámbito computacional.

El cuarto capítulo menciona la importancia de la formación de cualquier usuario de la computadora. Una de las maneras de prevención de virus informáticos es el tener un conocimiento informático abundante, y así poder tomar las mejores acciones de prevención para el ataque de un posible virus, como por ejemplo tener la capacidad de seleccionar el mejor antivirus para nuestra equipo de cómputo basándonos en nuestra plataforma informática.

Una vez obtenido dicho conocimiento informático, por consecuencia se tendrá una buena formación del usuario, de manera que podrá identificar cuando el equipo de cómputo presente alguno o varios síntomas de contagio derivados de un virus.

En el quinto capítulo se indican las acciones preventivas que se deben tomar para protegerse de las futuras amenazas y poder salvaguardar la información. También se desarrolla un plan de contingencia con el cuál se podrá eliminar un virus informático, una vez que se haya identificado dicha amenaza en el ordenador.

I

LA COMPUTADORA Y VIRUS INFORMÁTICOS

1.1 Historia de la Computadora

La historia de la computadora es muy interesante ya que muestra como el hombre logra producir las primeras herramientas para registrar los acontecimientos diarios desde el inicia de la civilización, como es que con el paso del tiempo la computadora va evolucionando logrando grandes alcances que jamás se hubiera logrado imaginar.

Cuando en las computadoras se habla de historia, se debe de comprender que desde sus inicios no se ha transcurrido ni medio siglo desde que se inventó la primera, por lo que hay que considerar otras formas de unidad de medida de su desempeño; lo cual anteriormente mencionado, significa que la corta cronología se debe medir no tanto en términos de años sino más bien en su función de sus avances tecnológicos.

Una computadora o también conocida como Ordenador es una máquina electrónica que recibe y procesa datos para convertirlos en información útil, la cual está compuesta por circuitos integrados y otros componentes relacionados que pueden ejecutar con exactitud, rapidez y eficacia. Los datos que recibe la computadora pueden venir ordenados por un usuario o en su defecto por un programa. Su característica principal que la distingue de otros dispositivos de similares como por ejemplo una calculadora, es que la computadora puede realizar tareas muy diversas cargando distintos programas en la memoria para que los ejecute el procesador y la calculadora únicamente puede realizar una función a la vez.

A lo largo del paso del tiempo y de las constantes evoluciones de la computadora, existen seis generaciones de estas, a continuación se mostrará en la tabla 1.1, los rasgos más sobresalientes en cada generación:

GENERACIONES DE LA COMPUTADORA

GENERACIÓN	PERIÓDO	CARACTERÍSTICAS
1a GENERACIÓN	1951 a 1958	- Las primeras computadoras empleaban bulbos o tubos al vacío para procesar información. - Los operadores ingresaban datos por medio de tarjetas perforadas. - Se programaban en lenguaje de máquina. - Algunas de las primeras máquinas fueron MARK I, ENIAC, EDVAC, UNIVAC E IBM 701.
2a GENERACIÓN	1959 a 1964	- Surgió el transistor lo cual hizo computadoras más rápidas y más pequeñas. - Las computadoras eran más pequeñas que la de bulbos. - Se usaban para reservaciones en líneas aéreas y simulaciones para uso general. - Se programaban con lenguaje alto nivel. - Algunas de las computadoras fueron UNIVAC M460, NCR 315, IBM 1401 Y HOEYWELL 800.
3a GENERACIÓN	1964 a 1971	- En esta generación se implementan los circuitos integrados en los cuales se colocan miles de componentes electrónicos. - Surge la multiprogramación (Computadora que puede procesar varios programas de manera simultánea) - Las computadoras se hacen más pequeñas, más rápidas y son más eficientes.
4a GENERACIÓN	1971 a 1981	- Aquí surgen los microprocesadores que son circuitos integrados de alta densidad y velocidad. - Aparecen otras aplicaciones como lo son procesadores de palabras, hojas de cálculo, paquetes gráficos. - Surgen las computadoras personales. - EL software de las computadoras hace más sencilla la interacción con el usuario.
5a GENERACIÓN	1982 a 1989	- Surge la Inteligencia Artificial y la Robótica. - Las computadoras se vuelven más livianas y con mayor velocidad de procesamiento. - Aparecen las supercomputadoras para cálculos científicos.
6a GENERACIÓN	1990 a 2011	- Las computadoras cuentan con cientos de microprocesadores vectoriales trabajando al mismo tiempo. - Algunas tecnologías ya han sido desarrolladas o están en proceso como lo son: inteligencia Artificial, Teoría del Caos, Transistores Ópticos, Sistemas difusos. - Las redes de área mundial (WAN) siguen creciendo usando a su vez el uso de fibra óptica y satélites, con lo cual se logran anchos de banda impresionantes.

Fuente: creación propia, 2012 TABLA 1.1

1.2 Arquitectura de la Computadora

La arquitectura de Von Neumann describe una computadora con 4 secciones principales: la unidad aritmético lógica (ALU por sus siglas del inglés: Arithmetic Logic Unit), la unidad de control, la memoria central, y los dispositivos de entrada y salida (E/S). Estas partes están interconectadas por canales de conductores denominados buses.

A pesar de que las tecnologías empleadas en las computadoras digitales han cambiado mucho desde que aparecieron los primeros modelos en los años 40, la mayoría todavía utiliza la Arquitectura de von Neumann, publicada a principios de los años 1940 por John Von Neumann.

La memoria es una secuencia de celdas de almacenamiento numeradas, donde cada una es un bit o unidad de información. La instrucción es la información necesaria para realizar lo que se desea con el ordenador. Las «celdas» contienen datos que se necesitan para llevar a cabo las instrucciones. El número de celdas varían mucho, y las tecnologías empleadas para la memoria han cambiado bastante; van desde los relés electromecánicos, tubos llenos de mercurio en los que se formaban los pulsos acústicos, matrices de imanes permanentes, transistores individuales a circuitos integrados con millones de celdas en un solo chip. En general, puede ser reescrita varios millones de veces (memoria RAM); se parece más a una pizarra que a una lápida (memoria ROM) que sólo puede ser escrita una vez.

El procesador (también llamado Unidad central de procesamiento o CPU) consta de manera básica de los siguientes elementos:

La unidad aritmético lógica o ALU es el dispositivo diseñado y construido para llevar a cabo las operaciones elementales como las operaciones aritméticas (+, - , * , /), operaciones lógicas (Y, O, N), y operaciones de comparación o relacionales, en esta unidad es en donde se hace todo el trabajo computacional.

La unidad de control sigue la dirección de las posiciones en memoria que contiene la instrucción que el computador va a realizar en ese momento; recupera la información poniéndola en la ALU para la operación que debe desarrollar. Transfiere luego el resultado a ubicaciones apropiadas en esta misma. Una vez que ocurre lo anterior, la unidad de control va a la siguiente instrucción (normalmente situada en la siguiente posición, a menos que la disposición sea una de salto, informando al ordenador de que la próxima solicitud estará ubicada en otra posición de la memoria).

Los procesadores pueden constar de además de las anteriormente citadas, de otras unidades adicionales como la unidad de Coma Flotante.

Los dispositivos de Entrada/Salida sirven a la computadora para obtener información del mundo exterior y comunicar los resultados generados por el computador al exterior. Hay una gama muy extensa como teclados, monitores, memorias USB, cámaras web, etc.

1.3 Software y Hardware

Todas las computadoras sin excepción alguna están compuestas por un Hardware y a su vez por un Software.

¿Qué es el Hardware? Son todas aquellas partes tangibles de la computadora por mencionar algunos ejemplos está el monitor, el teclado, el mouse, la fuente, el disco duro, un router, un switch, el modem, etc.

¿Y qué es el Software? Son todos aquellos programas que se encuentran en la computadora. Son las instrucciones responsables de que el hardware realice su tarea de una forma correcta.

Como concepto general, el software puede dividirse en varias categorías basadas en el tipo de trabajo realizado. Las dos categorías primarias de software son los sistemas operativos (software del sistema), que controlan los trabajos del ordenador o computadora, y el software de aplicación, que dirige las distintas

tareas para las que se utilizan las computadoras. Algunos ejemplos de Software pueden ser Windows, Office, Linux, Juegos o un Antivirus.

Cabe señalar que el Software y el Hardware deben de funcionar en conjunto para que la computadora realice los trabajos que se le soliciten de una manera correcta. La evolución del Software y Hardware son constantes conforme pasan los años y muchas empresas se enfocan en la creación de más innovaciones para lanzarlas al mercado.

1.4 Sistema Operativo

El sistema operativo es el programa (o software) más importante de una computadora para que funcionen los otros programas, cada ordenador de uso general debe tener uno. Estos realizan tareas básicas, tales como reconocimiento de la conexión del teclado, enviar la información a la pantalla, no perder de vista archivos y directorios en el disco, y controlar los dispositivos periféricos tales como impresoras, escáner, etc.

El computador sólo entiende lo que conocemos como Lenguaje Máquina. (Marcelo, 2000).

En sistemas grandes, el sistema operativo tiene incluso mayor responsabilidad y poder, es como un policía de tráfico, se asegura de que los programas y usuarios que están funcionando al mismo tiempo no interfieran entre ellos. También es responsable de la seguridad, asegurándose de que los usuarios no autorizados no tengan acceso al sistema.

La filosofía de diseño de los sistemas operativos es en todo los casos, bastante parecida. En cuanto a las computadoras, las diferencias suelen estar en los microprocesadores. Actualmente los basados en la tecnología INTEL (PC´s) y los de Motorola (Macintosh), ocupan casi todo el mercado. En cuanto a los sistemas operativos en sí, una gran parte es ocupada por sistemas basados en el MS-DOS, y el resto en el UNIX. (Marcelo, 2000).

1.5 Internet

En palabras sencillas, la Internet es un conjunto de computadoras conectadas entre sí, compartiendo una determinada cantidad de contenidos; por este motivo es que no se puede responder a la pregunta de donde está la Internet físicamente - está en todas las partes donde exista un ordenador con conectividad a esta red. En términos más informáticos podríamos decir que el Internet es una red informática descentralizada, que para permitir la conexión entre computadoras opera a través de un protocolo de comunicaciones. Para referirnos a ella además se utiliza el término "web" en inglés, refiriéndose a una "tela de araña" para representar esta red de conexiones.

1.5.1 Formas de acceso a Internet

Podemos decir que Internet es una gran red o una red de redes, en la que existen un gran número de servidores. A estos nos conectamos mediante otros a los que contratamos ese servicio. Estos son los llamados ISP (Internet Service Provider o Proveedor de Servicios de Internet).

Existen diversas maneras para acceder a Internet, por mencionar algunos ejemplos de conexión se encuentra:

- Conexión por la red digital telefónica
- Conexión mediante cable
- Conexión de banda ancha
- Conexión WI-FI
- Conexión 3G
- Conexión GPRS

1.5.2 Evolución del Internet

Hoy en día, nadie se puede quedar fuera de esta red de redes. Esta está presente en casi todos los hogares del mundo, como en todas las empresas del globo, ya de manera obligatoria. Muchos estudios, trabajos y funciones empresariales, no se conciben sin el Internet. Así de simple. Incluso muchos gobiernos, se han puesto en campaña, para alfabetizar digitalmente a sus ciudadanos. Es que la tecnología y el Internet, ya llegaron y lo han hecho para quedarse y revolucionar de manera constante, nuestra forma de vida.

Con el paso de los años el internet a evolucionado ya que desde sus inicios el acceder a la red se veía como algo complicado para los usuario de la computadora, las tarifas de la empresas encargadas de brindar el servicio eran de costos excesivos, pero a estas alturas la tarifas se han vuelto más accesibles, y ya se accede al internet de una manera más fácil comparada con los primeros inicios del internet.

1.6 Virus informático

Con el término “virus” se designa un programa de ordenador, generalmente anónimo, que lleva a cabo acciones que resultan nocivas para el sistema informático. (Mur et al., 1990).

Un virus informático es un software malintencionado o llamado también con el nombre en inglés malware, que tiene por objetivo alterar el correcto funcionamiento de la computadora u ordenador, sin el permiso o el conocimiento del usuario. Los virus habitualmente reemplazan archivos ejecutables por otros infectados con el código de este. (Anónimo. *¿Qué es un Virus Informático?*, [Web en línea]. 2011).

Los virus informáticos básicamente tienen la función de propagarse, no se replican a sí mismos porque no tienen esa facultad para hacerlo como el gusano informático, los virus dependen de un software para propagarse y cabe señalar que son muy dañinos, algunos contienen distintos objetivos, como lo puede ser

desde abrir ventanas para realizar una simple broma a algún usuario hasta realizar grandes daños importantes en el sistema operativo o también bloqueando las redes informáticas para así generar tráfico.

Es importante destacar que **el potencial de daño de un virus informático no depende de su complejidad sino del entorno donde actúa**, por ejemplo, no es lo mismo tener una computadora infectada de un virus informático, que ésta a su vez tiene la función de brindar el servicio de correo electrónico de una empresa a una computadora infectada que se usa en el hogar.

1.7 Surgimiento de los virus

No se sabe exactamente cuál fue el primer virus en la historia de las computadoras, aunque sí se sabe cuál fue posiblemente el primero en una computadora con sistema operativo.

Los articulistas más escrupulosos otorgar la paternidad a John Von Neumann la paternidad de los virus. (Mur et al., 1990).

Algunos llevan este comienzo a los primeros conceptos de programas autoreplicantes, o sea programas que se reproducen, los cuales se describen en el trabajo: "Theory and Organization of Complicated Automata" de John Von Newman, ya en el año de 1942. En ese tiempo las computadoras se programaban con alambres (literalmente), es decir los programas eran conexiones que se hacían entre las diversas partes electrónicas de la computadora. Hasta que precisamente John Von Newman creó el concepto de "programa almacenado", en el cual los programas y datos se almacenan juntos en la memoria del ordenador. Esto dio una gran flexibilidad a las grandes computadoras de entonces, pero al poder modificar las instrucciones surgió también la posibilidad de "sabotear" el código fuente.

El código fuente es un conjunto de líneas de texto que son las instrucciones que debe seguir la computadora para ejecutar dicho programa. Por tanto, en el código fuente de un programa está descrito por completo su funcionamiento.

A finales de los años 50, en los laboratorios Bell, tres programadores, H. Douglas Mcllroy, Víctor Vysottsky y Robert Moris inventaron un juego llamado "Core Wars", el cual consiste en elaborar programas para una computadora ficticia simulada. El objetivo es que estos sobrevivan usando técnicas de ataque, ocultamiento y reproducción semejantes a los virus.

En la década del 70, aparecieron otros programas del mismo tipo. John Shoch y Jon Hupp, investigadores de Palo Alto Research Center (PARC) de Xerox aseguran que ya en 1970 habían elaborado softwares con ciertas técnicas virales de reproducción. Aunque estos podrían ser considerados virus buenos, por así decirles, ya que controlaban continuamente la salud de las redes.

A uno de ellos lo llamaron “El gusano vampiro" porque se escondía en la red y sólo se activaba en las noches para aprovechar las computadoras que no se estaban utilizando. También en 1970, en lo que eran los inicios de Internet, en ARPAnet la red militar y universitaria, un investigador llamado Bob Thomas liberó un programa llamado 'Creeper' (rastrero), el cual se arrastraba por toda la red desplegando este mensaje: "Soy el 'Rastrero', atrápame si puedes!". Otro programador escribió otro "virus" llamado "Reaper" (segador) el cual se reproducía en la red matando Creepers. Esos primeros virus no causaban daño o destrucción, sólo eran experimentos sobre ideas curiosas de programas que generaban copias de sí mismos.

Tal vez el primer virus, o al menos el primero en recibir esa denominación, fue ideado en noviembre de 1983. En un seminario sobre seguridad en computadoras a Fred Cohen se le ocurrió el experimento (en una minicomputadora VAX 11/750) de hacer un programa que "pudiera modificar otros para incluir una copia (posiblemente evolucionada) de sí mismo".

En mayo de 1984, en la revista "Scientific American", A.K.Dewdney en su sección "Computer Recreations" describe el juego "Core Wars" con lo que le da amplia difusión. Varios lectores escriben sus experiencias al experimentar con programas de tipo virus. Uno de ellos comenta: "Nunca conseguí eliminar completamente esa peste electrónica"

En enero de 1986 aparece el virus "Brain", originario de Paquistán, el que es considerado el primer virus para PCs con sistema operativo MS-DOS. Al principio no causaba daño, sólo mostraba un mensaje de advertencia: "Bienvenido al calabozo. (c)1986 Basit & Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES", luego la dirección y teléfono, y "Cuidado con este virus... Contáctenos para vacunarse...." (Museo de la Informática y Computación Aplicada. *Historia*, [Web en línea]. (2003-2010).

En la actualidad, los virus son producidos en cantidades extraordinarias por muchísima gente alrededor del planeta. Algunos de ellos dicen hacerlo por un afán de entretenimiento, 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. Para muchos los virus informáticos existen por una razón económica se cree que los propios fabricantes de software antivirus son los que propagan la infección para luego incrementar la venta de sus productos.

1.8 Características de los virus

No todos los virus presentan las mismas características pero en general tienen algunas similitudes, como las que se mencionan a continuación:

1.- Los virus pueden infectar múltiples archivos de la computadora infectada (y la red a la que pertenece): Debido a que algunos virus residen en la memoria, tan pronto como un disquete o programa es cargado en la misma, el virus se “suma” o “adhiere” a la memoria misma y luego es capaz de infectar cualquier archivo de la computadora a la que tuvo acceso.

Un virus intentará infectar el máximo de archivos para así iniciar una propagación por todo el computador en forma de progresión geométrica. (Marcelo, 2000).

2.- Pueden ser Polimórficos: Algunos virus tienen la capacidad de modificar su código, lo que significa que un virus puede tener múltiples variantes similares, haciéndolos difíciles de detectar.

3.- Pueden ser residentes en la memoria o no: Como lo mencionamos antes, un virus es capaz de ser residente, es decir que primero se carga en la memoria y luego infecta la computadora. También puede ser "no residente", cuando el código del virus es ejecutado solamente cada vez que un archivo es abierto.

4.- Pueden ser furtivos: Los virus furtivos (stealth) primero se adjuntarán ellos mismos a archivos de la computadora y luego atacarán el ordenador, esto causa que el virus se esparza más rápidamente.

5.- Los virus pueden traer otros virus: Un virus puede acarrear otro virus haciéndolo mucho más letal y ayudarse mutuamente a ocultarse o incluso asistirlo para que infecte una sección particular de la computadora.

6.- Pueden hacer que el sistema nunca muestre signos de infección: Algunos virus pueden ocultar los cambios que hacen, haciendo mucho más difícil que el virus sea detectado.

7.- Pueden permanecer en la computadora aún si el disco duro es formateado: Si bien son muy pocos los casos, algunos virus tienen la capacidad de infectar diferentes porciones de la computadora como el CMOS o alojarse en el MBR (sector de buteo). (Alegsa. *Características de los virus informáticos*, [Web en línea]. (1998-2011).

1.8.1 Módulos principales de un virus informático

Módulo de Reproducción: Sé 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 disimuladamente. 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.

Módulo de Ataque (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 daños, tiene un módulo de ataque que se activa cuando el reloj del ordenador indica 6 de Marzo. En estas condiciones la rutina actúa sobre la información del disco rígido volviéndola inutilizable.

Módulo de Defensa (optativo): Tiene 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. (Manson. *Estudio sobre virus informáticos*, [Web en línea]. (2011).

1.8.2 Tareas básicas de los virus

Los virus no se pueden activar por sí solos, por lo que dependen siempre de un fichero ejecutable que los cargue en memoria. Así, se establece un vínculo entre un virus y el programa al que se asocia, de tal forma que cuando este es ejecutado por el usuario el virus es cargado en memoria por el sistema operativo, a escondidas de este, y entonces es cuando puede desarrollar su acción contaminadora. Este programa anfitrión del virus puede ser desde un video juego hasta una simple macro, pasando por toda la gama de ficheros que contengan código ejecutable por parte del usuario o del sistema operativo. Cuando se arranca el programa asociado al virus, éste se carga en memoria junto con su anfitrión, y una vez cargado debe realizar dos tareas indispensables para él que son:

- Buscar otros programas ejecutables, discos duros o disquetes a los que infectar. Para ello debe disponer de una porción de código encargada de rastrear los discos duros y los disquetes, los programas de correo, los

ficheros que contengan macros, etc., buscando aquellos idóneos para ser contaminados.

- Autocopiarse, una vez detectado el programa o disco a infectar, el virus debe disponer de otra parte en su código capaz de realizar una copia de sí mismo en este nuevo anfitrión.

Además de estas tareas básicas, un virus puede también:

- Atacar de forma directa el equipo anfitrión: este ataque puede destruir la FAT del disco duro, borrar una parte o la totalidad del mismo, modificar o destruir ficheros importantes para el ordenador (ficheros del sistema, de configuración, atacar el registro, etc.), cambiar algún aspecto gráfico del sistema (mostrar una imagen o mensaje en pantalla, cambiar la disposición de los iconos del escritorio, etc.) y cualquier otra acción posible en el equipo.

- Modificar segmentos de su propio código, polimorfismo, cada vez que se copie: para de esta forma evadir la acción de los antivirus, creando mutaciones de sí mismo en cada copia. Algo análogo a lo que hacen los virus biológicos, como el de la gripe, que muta cada año, burlando con ello a las vacunas y medicamentos que se crean para atacarla y prevenirla.

- Autoencriptarse para así evitar la acción de los antivirus. Estos programas buscan cadenas determinados dentro de los ficheros del ordenador que escanéan, por lo que si el virus encripta su propio código se hará invisible a este proceso de detección.

1.8.3 Programación de un virus informático

El lenguaje de programación clásico para construir virus es el Ensamblador, ya que es un lenguaje de bajo nivel, idóneo para producir código máquina capaz de tomar el control sobre las interrupciones o de saltar de un programa a otro, pero también es posible programar virus en Visual Basic, C++, JavaScript, Java.

Otra característica común en la mayoría de los virus informáticos es que están formados por poca cantidad de código, ya que al tener un tamaño mínimo es fundamental para evitar ser detectados y eliminados.

Los virus suelen permanecer ocultos en una primera fase, tratan de esconderse mientras se reproducen, para no ser descubierto, para ello reorientan la lectura del disco, y se manifiestan en una segunda fase.

1.9 Ciclo de vida de un virus

El ciclo de virus de un virus empieza cuando es creado y termina cuando es completamente erradicado. A continuación se describe cada etapa:

- Creación (Programación y Desarrollo)

Hasta hace pocos años, crear un virus exigía tener un profundo conocimiento de un lenguaje de programación, en la actualidad cualquiera que tengo un poco de conocimientos en programación pude hacer un virus.

En esta etapa se inicia el proceso de programación del virus definiendo sus características de autorreproducción y sus rutinas que causará los daños al sistema.

- Gestación (Distribución e infección del sistema)

Después de que el virus es creado, el programador hace copias asegurándose de que se extienda. Generalmente esto se logra infectando un programa popular y luego enviándolo o distribuyendo copias en oficinas, colegios u otras organizaciones.
Una vez infectado el sistema ya sea por vía e-mail, discos flexibles, etc., se aloja en la memoria del ordenador para esperar una orden o instrucción que lo ejecute para poder causar los daños y multiplicarse.

- Reproducción y Propagación

Los virus se reproducen naturalmente, éste mismo, bien diseñado está preparado para estar copiándose a sí mismo en distintos ficheros durante bastante tiempo antes de activarse, lo cual permite que se propague por todos lados, lo suficiente para llegar a muchísimos usuarios.

- Activación (Inicio de actividad del virus)

Los virus que contienen rutinas dañinas, se activarán bajo ciertas condiciones, por ejemplo, en determinada fecha o cuando el usuario haga algo determinado. Los virus sin rutina dañina no se activan, pero causan daño al robar espacio en el disco.

- Descubrimiento

Cuando se detecta un nuevo virus, se aísla y se envía a la Asociación Internacional de Seguridad Informática, con sede en Washington D.C., donde se toma nota de sus características para posteriormente distribuirlo a los fabricantes de antivirus. En general, el descubrimiento tiene lugar por lo menos un año antes de que el virus se convierta en una amenaza para la comunidad informática.

- Asimilación

En este punto, quienes desarrollan los productos antivirus, modifican su programa para que éste pueda detectar los nuevos virus. Esto puede tomar de un día a seis meses, dependiendo de quién lo desarrolle y el tipo de virus.

- Erradicación

Cualquier virus puede ser erradicado si suficientes usuarios mantienen al día su protección antivirus. Hasta el momento ningún virus ha desaparecido por completo (a excepción de los que se autoeliminan después de cumplir un objetivo), pero algunos hace mucho que han dejado de representar una amenaza importante. (Seguridad Informática. “Ciclo de Vida de un Virus”, [Web en línea]. (2004-2011).

1.10 Métodos de Propagación

En la actualidad no existe una forma única ni general de propagación de un virus, teniendo en cuenta que cada uno en particular tiene su propio sistema de propagación.

Una característica esencial en la propagación de los virus la constituye su mecanismo de arranque. (Mur et al., 1990).

La activación de un virus es involuntaria. Muchos virus pueden evitarse con simples conocimientos del sistema operativo, o por lo menos les podemos hacer la vida más difícil. (Marcelo, 2000).

1.11 Formas de Infección

En sus primeros tiempos, la vía principal de expansión de los virus eran los discos flexibles. Aquellos virus estaban incrustados en el sector de arranque del disquete, de tal forma que cuando se usaba el mismo como disco de inicio, o inadvertidamente arrancaba el ordenador con este introducido en la disquetera, el virus se hacía con el control de equipo, copiándose en el disco duro. Posteriormente, con la aparición de Internet, los CD-Roms, las memorias USB, etc., se han ampliado las formas de infección de un ordenador. A continuación se explican algunas de ellas:

1.11.1 Internet

La Red se ha convertido en el mayor medio de transferencia de información entre ordenadores, y en consecuencia, hoy es la mayor vía de entrada de virus. Sin embargo, Internet posibilita numerosas formas de intercambiar información, y cada una de ellas tiene unas características y un potencial de riesgo distinto.

1) E-mail

Es la vía de entrada preferida actualmente por los virus, ya que tienen una extrema capacidad de replicación y propagación.

Un correo infectado puede extenderse en cuestión de minutos a miles de ordenadores de todo el mundo.

2) Navegación por páginas WEB

Algunas de las tecnologías incluidas en estas páginas (Applets Java y controles ActiveX) son programas que pueden estar infectados por virus y contagiar a los usuarios. Además, los virus más recientes aprovechan posibles fallos de seguridad en los servidores que alojan las páginas Web. Otros virus redirigen a los usuarios a página Web ya infectadas.

3) Transferencia de ficheros (FTP)

FTP significa Protocolo de Transferencia de Ficheros, es un sistema que sirve para colocar documentos en otros ordenadores que estén en cualquier parte del mundo (upload) o para descargar ficheros de dichos ordenadores (download). Al descargar un fichero, éste se copia directamente en nuestro ordenador, con el consiguiente contagio en caso de contener virus.

1.11.2 Redes de Ordenadores

En la actualidad hay una clara tendencia hacia la conectividad entre los ordenadores, sobre todo en el ámbito empresarial, lo que ha multiplicado el número de vías de entrada disponibles para los virus.

1) Discos compartidos

Un ordenador puede contar con uno o varios discos duros a los que otros usuarios tienen acceso desde cualquier punto de la red. Este disco podría estar infectado y provocar la infección de otros ordenadores cuando éstos lo utilicen. Igualmente sucede a la inversa: si un ordenador contaminado utiliza un disco compartido, podría infectarlo y la infección se extenderá a los restantes equipos de la red.

2) Estaciones

Los usuarios conectados a una red informática realizan miles de transacciones de información diarias, tanto internas (con otros equipos de la red) como externas (conexión a otras redes de área local o extensa y conexión a Internet). Por lo tanto, cualquier fichero infectado con virus puede entrar y salir de la red a través de las estaciones, si no están convenientemente protegidas.

3) Servidores

Estos equipos son los que permiten el funcionamiento de la red, las conexiones entre las estaciones, la disposición de ficheros, la gestión del correo electrónico, las comunicaciones con el exterior, etc. Para conseguirlo, utilizan determinadas aplicaciones que pueden tener vulnerabilidades, aprovechadas por los virus. Si los servidores se infectan, pueden contagiar a todos los equipos de la red de forma muy rápida. A su vez, estos equipos pueden ser infectados desde una estación o desde otro servidor.

4) Servidores proxy y firewalls

Son los puntos por los cuales entra y sale toda la información de la red, conformando el perímetro de la red. A través de ellos pueden llegar o enviarse ficheros infectados que producirían el contagio tanto en los ordenadores de la red, como en los equipos de otra red externa a la que se conecte cualquiera de ellos.

1.11.3 Unidades de Disco y Almacenamiento

Las unidades de disco y almacenamiento son en los que se guardan programas, ficheros, mensajes de correo con ficheros adjuntos, ficheros comprimidos, ficheros descargados desde Internet, etc. Estos son alguno de los medios más usuales de propagación de los virus.

1) CD-ROM, Memorias USB, Memorias SD, Memoria M2, etc.

Su gran capacidad y versatilidad los convierte a estos discos y memorias en los de mayor amenaza potencial. Por su fácil manejo y transportabilidad son los más

usados entre los usuarios del ordenador por lo tanto es más susceptible poder contraer una infección de virus por estos medios.

2) Unidades de disco duro extraíbles

Los ordenadores cuentan con uno o varios discos duros instalados en el interior de su carcasa. Sin embargo, para trasladar todo su contenido a otros sistemas informáticos, existen unidades de disco duro extraíbles que pueden ser utilizadas físicamente en varios sistemas informáticos. Si la información contenida en estas unidades está infectada, contaminará a nuevos ordenadores.

3) Discos compartidos en red

Son unidades de disco que se encuentran físicamente en un ordenador concreto, pero cuyo contenido es accesible para el resto de equipos conectados en su misma red. Evidentemente, si el disco compartido está contaminado, extenderá la infección al resto de ordenadores.

1.12 Clasificación de los virus

Por lo general, los virus son clasificados teniendo en cuenta diferentes aspectos, tales como su origen, la técnica que el virus implementa para cumplir su tarea, los archivos que puede llegar a infectar, el tipo de daño causado, dónde se instalan, es decir el sistema operativo o plataforma que utiliza para realizar su función.

A continuación se muestra una clasificación de virus basada en varias de sus características más importantes, como pueden ser su forma de contaminar, de activarse o de las partes del ordenador infectado a las que ataca. Hay que destacar que es frecuente considerar como virus a otras entidades de software que igualmente atacan a un ordenador anfitrión, como por ejemplo, troyanos, gusanos, etc. Podemos distinguir fundamentalmente los siguientes tipos de virus:

- Virus de Sector de Arranque (Boot)

  Se instalan en el sector de arranque, el cual contiene la información sobre el tipo de disco, es decir, numero de pistas, sectores, caras, tamaño de la FAT,

sector de comienzo, etc., de los discos duros del ordenador infestado, guardando el sector original en otra parte del disco, con lo que cada vez que se arranca el equipo el virus se ejecuta y se carga en memoria.

- Virus de Archivo, Fichero o de Programa

Su método de trabajo consiste en copiar su código a un fichero sin infectar. Luego, cuando el usuario ejecuta el fichero, es el virus el primero en ponerse en marcha. La mayoría se limita a infectar ficheros ".EXE" o ".COM" (extensiones ejecutables), aunque también verse afectados los ".DLL" (librerías de código usadas por el sistema), ".CPL" (paneles de control), ".SCR" (salva pantallas) y ".HLP" (ayuda hipertexto para Windows), normalmente insertan el código del virus al principio o al final del archivo, manteniendo intacto el programa infectado.

- Virus de Tabla de Partición

Este tipo de virus infecta el sistema de archivos y directorios del disco duro, una de sus características más notables es que son difíciles de detectar y eliminar.

- Virus BAT

Este tipo de virus emplea ordenes de MS-DOS en archivos de proceso por lotes consiguen replicarse y efectuar daños como cualquier otro tipo virus. En ocasiones, los archivos de proceso por lotes son utilizados como lanzaderas para colocar en memoria virus comunes, para ello se copian a sí mismo como archivos ".COM" y se ejecutan. Aprovechar ordenes como @ECHO OFF y REM traducidas a código maquina son "comodines" y no producen ningún efecto que altere el funcionamiento del virus.

- Virus Multi-Partes

Son una mezcla entre los virus de sector de arranque y los de programa. Un ejemplo son los Virus Polimórficos; Este virus se oculta en un archivo y se aloja en

memoria en el momento en que dicho archivo es cargado, luego hace una copia de sí mismo pero esta copia no es exacta y cada vez que infecta un archivo el virus cambia, esto ha dificultado la detección y futura eliminación del virus.

- Virus del MIRC

Vienen a formar parte de la nueva generación de Internet y demuestra que la Red abre nuevas forma de infección. Consiste en un script para el cliente de IRC Mirc. Cuando alguien accede a un canal de IRC, donde se encuentre alguna persona infectada, recibe por DCC un archivo llamado “script.ini”.

- Gusanos (Worms)

Un gusano informático es un programa (o conjunto de programas) que utilizan copias completas de sí mismos para infectar distintos equipos informáticos, en los que dejan esa reproducción o un segmento suyo. Básicamente, los gusanos se limitan a realizar copias de sí mismos, sin tocar ni dañar ningún otro fichero, pero se reproducen a tal velocidad que pueden colapsar por saturación las redes en las que se infiltran. Principalmente se extienden a través del correo electrónico, como los conocidos “I Love You“, “Navidad”, “Pretty Park”, “Happy99”, “ExploreZip”.

- Troyano o Caballo de Troya

Un caballero de Troya o troyano (Trojan en inglés) es un programa que lleva a cabo acciones inesperadas o no autorizadas, a menudo dañinas, como mostrar mensajes en pantalla, borrar archivos o formatear discos. Los troyanos no infectan otros archivos introduciéndose en ellos, por lo que no hace falta limpiarlos. Se introduce y camufla bajo la apariencia de información extraviada o simple basura. Se diferencian de los virus en que no se reproduce infectando otros ficheros. Tampoco se propaga haciendo copias de sí mismo como hacen los gusanos.

1.13 Métodos de Protección

Los métodos para contener o reducir los riesgos asociados a los virus se pueden clasificar en dos tipos, denominados activos y pasivos. Los métodos pasivos los

conocemos también como Sistema de Prevención y Los métodos activos se les conoce también como Métodos de Detección. (Marcelo, 2000).

En la tabla 1.2 se muestran las características de cada uno de ellos:

MÉTODOS DE PROTECCIÓN

ACTIVO	Antivirus: Son programas que 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 archivos: Consiste en generar filtros de archivos dañinos si la computadora está conectada 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.
PASIVO	- Evitar introducir al equipo medios de almacenamiento removibles que se sospechen estar infectados. - No instalar software "pirata". Evitar programas que incluyan crack, generadores de claves, números serie, etc. - Evitar descargar software gratis de Internet de sitios que no demuestren información clara de su actividad y de sus productos o servicios. - No abrir mensajes provenientes de una dirección electrónica desconocida, o con alguna promoción muy tentadora, o con imágenes o nombres muy sugerentes. - Realizar copias de seguridad y tratar de automatizar la recuperación del sistema, es la mejor alternativa ya que nunca se está 100% libre de infección.

Fuente: creación propia, 2012 TABLA 1.2

1.14 Los virus más relevantes

A lo largo de la historia han existido y seguirán existiendo miles y millones de virus informáticos pero siempre se debe de tomar en cuenta a los más peligrosos; que si bien es recomendable tener conocimiento de todos pero por su gran existencia es imposible, no está demás tener una idea de los virus que tuvieron más relevancia por la gran magnitud de su peligrosidad.

A continuación se muestra una lista de los 10 virus más peligrosos de la historia:

1. Pakistani Brain. Apareció en 1986 y fue diseñado con la intención de distribuir publicidad de una compañía de software. Se colocó en diskettes, desde donde realizaba la infección del equipo.

2. Morris Worm. Apareció en 1988 y fue R. Morris, un estudiante, quien lo creó. Tiene el dudoso honor de ser el primer gusano informático que se movía libremente por la web.

Se estima que en ese momento el existían unos 60.000 ordenadores conectados a la red y Morris Worm logró infectar a 6.000, incluido el centro de investigación de la NASA.

3. W95/CIH. Su nombre está relacionado con la fecha del accidente nuclear de Chernobyl, y es comprensible si recordamos que los daños que ocasionó suman más de 800 millones de dólares. Lo único que se sabe de este virus es que nació en Taiwán aproximadamente en el 1998.

4. Melissa. Atacó a miles de usuarios y empresas el 26 de marzo de 1999. Se esparció a través de un documento de Microsoft Word infectado.

5. I love You. Este virus fue detectado en mayo de 2000, cuando infectó a miles de ordenadores en el mundo. Fue especialmente virulento con los sistemas operativos del “Pentágono” en EEUU.

Los daños que causó este malware creado en Hong Kong superan los 10 millones de dólares.

6. Code RED. Bautizado con el nombre de un popular refresco, este virus se propagaba sin necesidad de un correo electrónico o una página web. Localizaba ordenadores vulnerables y los dañaba aprovechando la fragilidad en un componente del Index Server de Microsoft. Afectó a 400.000 sitios red.

7. SQL Slammer. Infectó principalmente a equipos con Microsoft SQL Server, usado habitualmente para realizar tareas relacionadas con registros y bases de datos. Apareció en 2002, su origen a fecha de hoy sigue siendo desconocido.

8. Bagel-Netsky. Para muchos antivirus fue imposible detenerlo cuando apareció en 2004. Eran dos gusanos que se propagaban por medio de correo electrónico o a través de sitios de Internet infectados, los cuales buscaban crear conflictos en los equipos.

9. Sasser. Es un gusano que se propagó usando la vulnerabilidad en el proceso Local Security Authority Subsystem (LSASS por sus siglas en inglés). Sólo afectó a equipos Windows 2000/XP y Windows Server 2003 sin actualizar.

10. Storm Worm. Fue modificado cientos de veces, creando eventualmente la Bot-net más grande del mundo. En un momento se creyó que más de 15 millones de equipos fueron infectados al mismo tiempo, y que estaban bajo el control de los criminales.

La primera vez que se dejó ver fue en el año 2007. (Norton. *Los diez virus informáticos más peligrosos de la historia*, [Web en línea]. (2011).

El día de hoy se dio a conocer un nuevo malware que circula en la red llamado Duqu, este malware utiliza la función de un troyano para poder robar información del sistema.

Los laboratorios de BitDefender advirtieron esta semana sobre la aparición de un malware identificado como Duqu, el cual parece ser una nueva versión del denominado Stuxnet, diseñado para sabotear el programa nuclear de Irán en 2010.

La amenaza fue detectada a media semana, cuando los laboratorios identificaron al programa maligno como Win32.Duqu.A el cual resultó ser uno de los millones de ejemplares que recibieron los laboratorios de la empresa especialista en

antimalware. (Yahoo! News Network. *Alertan sobre aparición de nuevo malware*, [Web en línea]. (23 de Octubre de 2011).

1.15 Hacker, Cracker, Lamer, Newbie y Phreaker

En la actualidad existen diversos términos informáticos para referirse a las personas que más conocimiento poseen acerca de los computadores, que si bien en algunos casos dichas definiciones pueden ser parecidas entre sí, no lo son y es aquí donde la mayoría de la gente suele confundirlos y no saber distinguir las características que los distinguen.

A continuación se muestran los términos más comunes y mayormente empleados en el ámbito computacional así como sus respectivas definiciones:

- Hacker

Son usuarios expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones, dominan la programación y la electrónica para lograr comprender sistemas tan complejos como la comunicación móvil.

- Cracker

Cracker viene del inglés “crack” que significa romper y justamente es lo que estos usuarios hacen. Tienen más o menos los mismos conocimientos que los hackers pero no comparten la misma ética, por lo tanto ellos pueden borrar, modificar o romper un sistema una vez dentro.

- Lamers

Son usuarios con ganas de hacer hacking, pero carecen de cualquier conocimiento computacional. Con la oportunidad de buscar en internet estos usuarios buscan y recolectan información para poder entrar a un sistema. Este

grupo puede ser peligroso ya que ponen en práctica todo software de hackeo que encuentren en la red.

- Newbies

Este es un novato que navega por internet y llega a encontrarse con una página de hacking y descarga programas de hackeo. Al contrario que los lamers, los newbies aprenden el hacking siguiendo todos los pasos para lograrlo de manera que puedan ir aprendiendo.

- Phreaker

Estos usuarios son conocidos por sus conocimientos en la telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles.

II

ANTIVIRUS

2.1 ¿Qué es un Antivirus?

Es un 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. (Anónimo. *¿Qué es un antivirus?*, [Web en línea]. (2001-2011).

Los antivirus son programas dirigidos contra tipos particulares de virus informáticos. (Nombela *et al*., 1991).

En pocas palabras un antivirus es un programa cuya función es detectar y eliminar virus informáticos y otros programas maliciosos (a veces llamados malware).

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les han agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como heurística) o la verificación contra virus en redes de computadoras. Actualmente existe una nueva tecnología basada en Inteligencia Artificial llamada TruPrevent que cuenta con la capacidad de detección de virus desconocidos e intrusos.

Un antivirus normalmente tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados, en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que suelen ejecutarse en un navegador web como por ejemplo: Active X o JavaScript.

La eficacia de estos programas antivirus dependerá en buena parte de una actualización permanente de los ficheros con los ficheros de “firmas” de nuevos virus, así como del soporte proporcionado por la empresa desarrolladora del programa instalado. (Gómez, 2007).

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.

- **Detector** 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 desarman 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. (Anónimo. *¿Qué es un antivirus?*, [Web en línea]. (2001-2011).

2.2 Historia de los Antivirus

Los virus informáticos están ligados con los antivirus ya que gracias a la aparición de dichos virus surgió la necesidad de poderlos erradicar, entonces se podría comentar que la primera aparición de un programa antivirus fue cuando surgió el primer virus.

Entonces con la aparición del primer virus llamado Creeper que atacó la computadora IBM SERIE 360 en el año de 1972, surgió el primer antivirus llamado Reaper.

También se conoció uno de los primeros antivirus llamado Full Shot (Inyección para la gripe y fue creado por un programador americano llamado Ross Greenberg.

Así surgió una industria dedicada a la defensa de los virus informáticos, lo que provocó el nacimiento de la llamada por sus siglas CVIA (Computer Virus Industry Association).

A partir de entonces se empezaron a desarrollar herramientas de detección y erradicación de los virus, lo cual desencadenó un mayor esfuerzo por parte de los creadores de virus para evitar su detección mediante los antivirus.

Es evidente que los antivirus imponen una seria limitación a la capacidad de propagación de un virus, y constituyen una útil herramienta para defendernos de los tipos de virus más conocidos. (Nombela *et al*., 1991).

2.3 Funcionamiento de los Antivirus

Existen diversas maneras de funcionamiento de los programas antivirus, esto dependiendo del fabricante o compañía que lo creó, pero en general todos los antivirus operan de una misma forma para poder realizar su adecuado funcionamiento. Se explicarán las diversas estrategias de operación de los antivirus, para la detección de códigos malignos.

- SCANNING (ESCANEAR)

Está basado en el reconocimiento de firmas de códigos malignos, utilizando para ellos una base de datos de virus conocidos. El problema de esta alternativa es que le continuo crecimiento de la base de datos de los virus (en algunos casos ya supera las 100,000 firmas de códigos malignos) puede afectar el rendimiento del sistema ya que el antivirus consume cada vez mayores recursos a medida que se va actualizando la base de datos.

- MONITOR RESIDENTE

Permite ofrece una protección en tiempo real, analizando cualquier archivo antes de que sea utilizado (copiar, ejecutar, instalar) o al ser descargado de Internet. Pero esta alternativa presenta el inconveniente de una mayor carga del sistema, así como de ocasionar posibles interferencias con otros servicios instalados, ya que el antivirus se encarga de interceptar y monitorizar todas las llamadas al sistema y la gestión de interrupciones en el equipo.

- ANÁLISIS HEURÍSTICO

Basado en la experiencia que permite detectar virus nuevos al reconocer código con un comportamiento sospechoso. En este caso, el problema podrían venir a consecuencias de falsos positivos, es decir, de ficheros legítimos que puedan ser detectados como virus por el programa antivirus.

- INTEGRITY CHECKING (COMPROBACIÓN DE LA INTEGRIDADA)

También conocida como “Vacunación de Ficheros”. En este caso el antivirus se encarga de generar una base de datos con una suma de control o código de integridad de cada archivo del sistema, para de este modo poder detectar y alertar al usuario de cualquier cambio en el tamaño de los archivos. Sin embargo, hay que tener en cuenta que algunos virus ya tienen en cuenta una posibilidad y tratan de engañar al sistema ofreciendo información falsa sobre el tamaño y el código de comprobación del fichero infectado.

- ANÁLISIS DEL COMPORTAMIENTO

Este trata de detectar todas las acciones sospechosas o potencialmente peligrosas que se realicen en el sistema informático como por ejemplo, escribir en el sector de arranque del disco duro, modificar un fichero ejecutable, etc.

2.4 Estructura de un Antivirus

La estructura de un programa antivirus, está compuesta principalmente por dos módulos: el primero denominado de control y el segundo denominado de respuesta, como se muestra en la tabla 2.1:

MÓDULOS DE ANTIVIRUS

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. Un algoritmo es una secuencia finita de instrucciones, reglas o pasos que describen de forma precisa las operaciones de un ordenador debe realizar para llevar a cabo un tarea en un tiempo más finito. [Donald E. Knuth, 1968] Algunos ejemplos de sus funciones son: ❖ Seguimiento de la actividad en el sistema informático ❖ Protección preventiva del sistema informático ❖ Detección de códigos malignos ❖ Configuración del funcionamiento del antivirus
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. Algunos ejemplos de sus funciones son: ❖ Generación de alarmas y registro de incidencias ❖ Bloqueo de registros y programas sospechosos ❖ Desinfección de archivos y programas

Fuente: creación propia, 2012 TABLA 2.1

2.5 Tipos de Antivirus

Existen diferentes tipos de antivirus o de diversas formas de presentación, con la siguiente tabla se explicará y analizarán las diferencias entre cada uno de ellos.

Asimismo existen otras formas de presentarse este tipo de antivirus, algo que ya no depende de nosotros sino más bien de las ofertas y propuestas que muchos desarrolladores de software nos ofrecen, de allí que es gran parte de nuestro criterio y análisis el que tiene que decidir para saber cuál utilizar en un momento dado.

2.5.1 Antivirus Pasivo

Programa antivirus que se encuentra instalado en la computadora pero que no está en ejecución ni en protección permanente. Los antivirus online son ejemplos de antivirus pasivos. Por lo general se llega a usar cuando se quiere instalar algún software ilegal.

2.5.2 Antivirus Activo

Programa antivirus que se encuentra en ejecución en una computadora. Un antivirus activo no necesariamente tiene que estar en el proceso de escaneo del sistema ni tampoco en el estado de protección permanente (aunque esto último es recomendable para el antivirus activo). En general en una computadora no debería haber dos antivirus activos al mismo tiempo, porque pueden surgir conflictos o peor aún, anular la protección. Sí es posible tener un antivirus activo y varios inactivos.

Los antivirus inactivos podrían ejecutarse manualmente solo en determinadas situaciones, como por ejemplo, el antivirus activo no logra detectar un virus y se ejecuta un antivirus pasivo para su eliminación.

2.5.3 Antivirus On-Line

Programa antivirus que, en lugar de estar instalado y ejecutándose de forma permanente en el sistema, funciona a través de un navegador web.

Ventajas:

* Constante actualización: ya que la actualización de los antivirus depende directamente de la empresa desarrolladora del mismo.

* Alta disponibilidad y rapidez: no requieren una instalación completa en el sistema y pueden ser ejecutados rápidamente en cualquier momento usando el navegador. Muy buena alternativa para cuando el antivirus offline no detecta o no puede eliminar un programa maligno.

* Escaneo del sistema con múltiples antivirus: posibilidad de utilizar varios antivirus online sin afectarse entre sí. Porque, en general, no pueden instalarse dos o más antivirus offline en un mismo sistema.

* Suelen ser gratuitos.

Desventajas:

* Falta de eficacia y eficiencia: por el momento no son tan completos como los antivirus que se instalan en la computadora.

* Sin protección permanente: carecen de la función de protección permanente, suelen terminar cuando se cierra el navegador.

* Sólo escanean: Únicamente escanean la computadora en búsqueda de virus. No protegen áreas sensibles del sistema, ni tienen módulos especiales para control del tráfico de e-mails, mensajería o similares.

2.5.4 Antivirus Off-Line

Es el típico programa de antivirus que es instalado en un sistema y funciona de forma permanente en el mismo. Contrasta con los antivirus online, que funcionan generalmente a través de un navegador por internet.

Por el momento los antivirus offline suelen ser más poderosos, más efectivos y más eficientes que los antivirus online.

2.5.5 Antivirus Free

Es cualquier aplicación antivirus que no tiene costo alguno para quien lo usa. Son una alternativa a los antivirus de paga que requieren una licencia.

En general no suelen ser tan completos y potentes como los antivirus de pago, pero algunos de los antivirus gratuitos sorprenden por su capacidad de detección de virus, constantes actualizaciones y opciones disponibles.

2.5.6 Antivirus con Licencia

Estos softwares de antivirus vienen a ser de pago, no todos tienen las mismas funciones de protección de nuestro sistema operativo, razón por la cual hay que saber diferenciar y comparar entre las diferentes versiones que existen en el mercado, para así tomar la mejor decisión que creamos pertinente para la protección de nuestro sistema.

2.6 Complementos de un Antivirus

Los programas de Antivirus además de ofrecer una protección en contra de los Virus Informáticos, se complementan con otras funciones las cuales nos brindan una mayor protección a nuestro equipo de cómputo.

Estos complementos hacen que los usuarios tomen la decisión de elegir, entre diversos softwares de antivirus, ya que ofrecen un rango más amplio de seguridad del sistema operativo, brindando así al usuario una mayor tranquilidad al momento de usar su equipo.

Por mencionar algunos de estos complementos se encuentran, el Firewall, Anti-Spam, Anti- Spyware, entro otros. A continuación se muestra la descripción de algunos de ellos.

2.6.1 Anti-Spyware

El spyware es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador, entonces el complemento Anty-Spyware impide esta función ya que busca, detecta y elimina spywares en el sistema.

2.6.2 Anti-Spam

El principal objetivo de una herramienta antispam, es lograr un buen porcentaje de filtrado de correo no deseado. Pero tampoco deben identificar al correo deseado como no deseado, pues eso traería peores consecuencias que "olvidar" filtrar algún spam. Las herramientas antispam utilizan múltiples técnicas para detectar el correo no deseado como por ejemplo la técnica local y la no local.

2.6.3 Firewall

Es una herramienta que funciona como sistema de defensa, que evita cualquier tipo de acceso a un determinado sistema.

Estos programas suelen usarse para la protección de una computadora que está conectada a una red, especialmente a Internet. Controlan todo el tráfico de entrada y de salida, informando o evitando actividades sospechosas. Algunos cortafuegos tienen capacidad de detectar espías y pop-ups.

2.6.4 Antipop-ups

Herramienta encargada de detectar y evitar que se muestren los pop-ups y ventanas similares mientras se navega por la web. Existen diferentes tipos de antipop-ups, con diferentes resultados. En general permiten bloquear los pop-ups avisando de alguna manera al usuario cuando ciertas ventanas son bloqueadas.

Algunos antipop-ups vienen incorporados a los navegadores, cortafuegos y antivirus.

2.6.5 Anti-rootkits

Herramientas usadas frecuentemente por los intrusos informáticos o crackers con el objetivo de acceder ilícitamente a un sistema informático. Hay rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Microsoft Windows. Por ejemplo, el rootkit puede esconder una aplicación que lance una consola cada vez que el atacante se conecte al sistema a través de un determinado puerto. Los rootkits del kernel o núcleo pueden contener funcionalidades similares.

2.7 Antivirus populares y sus características

Como se mencionó con anterioridad existen diversos tipos de software antivirus y con ello cada uno tiene sus diferentes características que lo hacen más efectivo o vulnerable. En el mercado informático existen ciertas preferencias de los usuario por ciertos software de antivirus ya sea por recomendación de otro usuario, por la publicidad que llega a tener cierto antivirus, porque tiene un periodo de prueba, por ser gratuito, etc.

A continuación se muestran algunos de los antivirus más usados en la actualidad:

- avast! Free Antivirus
- ESET NOD32 AntiVirus
- AVG Anti-Virus
- Avira AntiVir Personal 10.2.0.94
- Norton AntiVirus 2012
- Kaspersky Anti-Virus 2012 12.0.0.374
- Panda Cloud Antivirus 1.5.1 Free
- Microsoft Security Essentials (MSE)
- McAfee AntiVirus Plus 2011
- BitDefender Antivirus 2012
- G Data Antivirus 2012 22.0.6.1
- Comodo Antivirus 5.4.189822.1355 (32 / 64 bits)

- PC Tools Antivirus 2011 8.0.0.653 Edición Gratuita
- Dr.Web Anti-virus 4.33.2
- ZenOK Free Antivirus 2011 1.0.9
- Kingsoft Antivirus 2010.11.6.318
- PC Tools Spyware Doctor con Antivirus
- ClamWin Antivirus

(Softonic International S.L. *Antivirus*, [Web en línea]. (1997-2011).

III

SEGURIDAD, MÉTODOS DE PROTECCIÓN Y SISTEMA OPERATIVO

3.1 Tipos de Protección

Existen diversas formas de proteger un equipo de cómputo, de las diversas amenazas que circulan en el ámbito de la informática.

En la actualidad existen dos tipos de protección al sistema operativo, sus características se muestran en la tabla 3.1:

TIPOS DE PROTECCIÓN

PROTECCIÓN PASIVA	La protección pasiva o Sistema de Prevención como su nombre lo menciona se encarga de tomar las medidas preventivas para así poder evitar el ataque de un posible malware al equipo de cómputo. Medidas de protección son: • Crear copias de seguridad de nuestro sistema operativo • Tener particiones lógicas del disco duro • No introducir cualquier tipo de hardware al equipo • Tener licencias del software que se vaya a instalar • No abrir mails de procedencia desconocida
PROTECCIÓN ACTIVA	La protección activa se encarga de estar protegiendo nuestro sistema operativo en cualquier momento que se esté ejecutando, un ejemplo de protección activa y el más comúnmente usado es el uso del software antivirus pero existen otras maneras de protección como lo son: • Empleo de contraseñas para las diferentes sesiones del sistema operativo • Detectores genéricos (vigilan el tamaño de los archivos ejecutables). • Encriptar datos • Detectores de macros • Filtros de ficheros

Fuente: creación propia, 2012 TABLA 3.1

3.2 Vacunas

Las vacunas tienen como objetivo el intentar prevenir la infección de los virus antes que llegue a producirse.

Un programa vacuna se instala al encender el ordenador y queda residente en memoria. (Nombela *et al*., 1991).

Podemos mencionar con lo anteriormente señalado que las vacunas es un eficaz instrumento de protección, que nos protege contra casi cualquier tipo de virus informático.

Cabe señalar que existen diferentes tipos de vacunas, las cuales se muestran en la tabla 3.2:

TIPOS DE VACUNAS

VACUNAS	ACCIÓN, FUNCIÓN, ACTIVIDAD
SOLO DETECCIÓN	Son vacunas que solo detectan archivos infectados sin embargo no pueden eliminarlos o desinfectarlos.
DETECCIÓN Y DESINFECCIÓN	Son vacunas que detectan archivos infectados y que pueden desinfectarlos.
DETECCIÓN Y ABORTO DE LA ACCIÓN	Son vacunas que detectan archivos infectados y detienen las acciones que causa el virus
COMPARACÓN DE FIRMAS	Son vacunas que comparan las firmas de archivos sospechosos para saber si están infectados. Una firma digital es una marca de seguridad electrónica que puede agregarse a los archivos. Permite comprobar el editor de un archivo y ayuda a comprobar que el archivo no haya cambiado desde

	que se firmó digitalmente. (Microsoft Corporation, 2011)
COMPARACIÓN DE FIRMAS DE ARCHIVO	Son vacunas que comparan las firmas de los atributos guardados en tu equipo.
POR MÉTODOS HEURÍSTICOS	Son vacunas que usan métodos heurísticos para comparar archivos. En los productos antivirus se conoce como heurística a las técnicas que emplean para reconocer códigos maliciosos (virus, gusanos, troyanos, etc.) que no se encuentren en su base de datos (ya sea porque son nuevos, o por no ser muy divulgados). El término general implica funcionalidades como detección a través de firmas genéricas, reconocimiento del código compilado, desensamblado, desempaquetamiento, entre otros. (Wikipedia, 2011).
INVOCADO POR EL USUARIO	Son vacunas que se activan instantáneamente con el usuario.
INVOCADO POR LA ACTIVIDAD DEL SISTEMA	Son vacunas que se activan instantáneamente por la actividad del sistema.

Fuente: creación propia, 2012 TABLA 3.2

3.3 Filtros de Ficheros

Los filtros de ficheros se implementan cuando equipo u ordenador está conectado a una red, y la implementación de los mismos consiste en generar filtros de ficheros dañinos.

Este sistema de protección proporciona una seguridad en donde no se requiere la intervención del usuario. Por ejemplo estos filtros pueden usarse en el sistema de correos o usando técnicas de firewall.

3.4 Copias de Seguridad

Una forma más de protección o prevención de nuestro Sistema Operativo es la creación de respaldo de toda nuestra información.

En informática una copia de seguridad tiene como fin que estas mismas puedan utilizarse para restaurar el original después de una eventual pérdida de datos. (Wikipedia. *Copia de Seguridad*, [Web en línea]. (10 de Octubre de 2011).

Como ya sabemos en cualquier momento puede surgir el ataque de cualquier virus informático el cual si no se ataca con las herramientas adecuadas puede llegar a borrar nuestro sistema junto con toda nuestra información, es por eso que es indispensable contar con copias de seguridad para evitar esta catástrofe y no solo como medida de prevención para un ataque de cualquier virus, sino también como prevención para cualquier cataclismo, como por ejemplo algún desastre natural, un accidente con el equipo de cómputo, etc.

3.5 Ataques en al ámbito informático

Como se mencionó con anterioridad la creación y evolución de los virus informáticos es constante día con día, es por eso que una forma de protección contra cualquier tipo de amenaza es el estar actualizado con la información y noticias acerca de los ataques más peligrosos que circulan en la red.

Como usuario se debe de tener por lo menos una idea de estos ataque para así de alguna manera poder prevenir algún contratiempo, por ejemplo, si en esos momentos se encuentra un virus muy agresivo en la red que su característica de propagación sea por medio de correos, entonces eso nos da la pauta a tener mayor precaución al momento de abrir nuestro correo, aunque cabe añadir que esas medidas de prevención deben de ser siempre constantes.

3.6 Sistema Operativo

Existen grandes impactos dañinos que repercuten en nuestro sistema operativo por la introducción de algún virus informático o cualquier malware. Pero cabe señalar que así como existen diversos tipos de virus con sus características particulares, estos mismos son creados para atacar a ciertos Sistemas Operativos, es decir, no todos los virus que existen hoy en día son compatibles con todos los Sistemas Operativos de nuestro ordenador.

Un Sistema Operativo es el software encargado de ejercer el control y coordinar el uso del hardware entre diferentes programas de aplicación y los diferentes usuarios. Es un administrador de los recursos de hardware del sistema.

Es un sistema que consiste en ofrecer una distribución ordenada y controlada de los procesadores, memorias y dispositivos de E/S entre los diversos programas que compiten por ellos. (EURAM. *¿Qué es un Sistema Operativo?*, [Web en línea]. (2000).

Las funciones básicas del Sistema Operativo son administrar los recursos de la máquina, coordinar el hardware y organizar archivos y directorios en dispositivos de almacenamiento. (Masadelante.com. *¿Qué es un Sistema Operativo?*, [Web en línea]. (1999-2011).

El computador solo entiende lo que conocemos como Lenguaje Máquina. Para un ser humano sería horrible tener que utilizar este lenguaje para todo tipo de acciones a realizar en el computador. Por ello el sistema operativo se dedica a decir las órdenes del usuario a lenguaje máquina, y las respuestas del computador a mensajes más claros. (Marcelo, 2000).

Una vez que se explicó mejor el término de lo que es y hace un sistema operativo en pocas palabras podremos resumir que este mismo es el que nos ayuda a tener comunicación de un ser humano a una computadora.

3.7 Diferencia entre Sistema Operativo y Plataforma Informática

Si bien es cierto que para que un Sistema Operativo funcione correctamente tiene que estar instalado sobre una plataforma informática óptima, para su correcto funcionamiento, pero muchas veces se llega a mal interpretar estos dos conceptos, ya que si bien es cierto que estos dos tienen una similitud importante, esto no quiere decir que signifiquen lo mismo.

Una Plataforma Informática es un sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible. Dicho sistema está definido por un estándar alrededor del cual se determina una arquitectura de hardware y una plataforma de software (incluyendo entornos de aplicaciones). Al definir plataformas se establecen los tipos de arquitectura, sistema operativo, lenguaje de programación o interfaz de usuario compatibles.

Ejemplos de plataformas son IBM-PC, que incluye las arquitecturas I386 (X86), IA64 o AMD64 (x86-64); Macintosh, que incluye la arquitectura Gecko y PowerPC; y SPARC. Existen programas multiplataforma, que permiten ejecutarse en diversas plataformas. También existen emuladores, que son programas que permiten ejecutar desde una plataforma programas de otra emulando su funcionamiento. (Wikipedia. *Plataforma Informática*, [Web en línea]. (06 de Octubre de 2011).

Podemos decir que, un sistema operativo es el software que opera en el hardware para hacerlo funcionar, pero la plataforma es la base para que el hardware funcione.

3.8 Clasificación de los Sistemas Operativos

Los sistemas operativos pueden ser clasificados de la siguiente forma:

- ✓ Sistema Operativo Multitarea: Permite que varios programas se ejecuten al mismo tiempo.

- ✓ Sistema Operativo Monotareas: Estos son más primitivos y es todo lo contrario al mencionado anteriormente, es decir, solo pueden manejar un proceso en cada momento o que solo puede ejecutar las tareas de una en una.

- ✓ Sistema Operativo Monousuarios: Son aquellos que nada más puede atender a un solo usuario, gracias a las limitaciones creadas por el hardware, los programas o el tipo de aplicación que se esté ejecutando.

- ✓ Sistema Operativo Multiusuario: Permite que dos o más usuarios utilicen sus programas al mismo tiempo. Algunos sistemas operativos permiten a centenares o millares de usuarios al mismo tiempo.

- ✓ Secuencia o Procesamiento por Lotes: Es la ejecución de una lista de comandos del sistema operativo uno tras otro sin intervención del usuario. También puede referirse al proceso de almacenar transacciones durante un cierto lapso antes de su envío a un archivo maestro, por lo general una operación separada que se efectúa durante la noche.

- ✓ Tiempo Real: Un sistema operativo en tiempo real procesa las instrucciones recibidas al instante, y una vez que han sido procesadas muestra el resultado. Este tipo tiene relación con los sistemas operativos monousuarios, ya que existe un solo operador y no necesita compartir el procesador entre varias solicitudes.

- ✓ Tiempo Compartido: El tiempo compartido en ordenadores o computadoras consiste en el uso de un sistema por más de una persona al mismo tiempo. El tiempo compartido ejecuta programas separados de forma concurrente, intercambiando porciones de tiempo asignadas a cada programa (usuario). En este aspecto, es similar a la capacidad de multitareas que es común en la mayoría de los microordenadores o las microcomputadoras. Sin embargo el tiempo compartido se asocia generalmente con el acceso de varios usuarios a computadoras más grandes y a organizaciones de servicios,

mientras que la multitarea relacionada con las microcomputadoras implica la realización de múltiples tareas por un solo usuario.

3.9 Ejemplos de Sistema Operativo

Como se indicó en los párrafos anteriores existen cuantiosos sistemas operativos en el ámbito informático, la elección para la utilización de dicho sistema tiene que ver con la funcionalidad y las tareas a realizar.

Se detallan algunos ejemplos de sistemas operativos en la tabla 3.3:

TIPOS DE SISTEMAS OPERATIVOS

FAMILIA WINDOWS	❖ Windows XP ❖ Windows Server 2003 ❖ Windows Mobile ❖ Windows Vista ❖ Windows 7
FAMILIA MACINTOSH	❖ Mac OS 8 ❖ Mac OS 9 ❖ Mac OS X
FAMILIA UNIX	❖ GNU/Linux ❖ System V ❖ Solaris ❖ UnixWare

Fuente: creación propia, 2012 TABLA 3.3

3.10 Evolución de los Sistemas Operativos

Se han desarrollado varios tipos de sistemas operativos con diferentes interfaces y categorías. Pero se observar que todos los sistemas operativos han sufrido cambios por parte de los programadores, y siguen evolucionando.

Los sistemas operativos empleados normalmente son UNIX, Macintosh OS, MS−DOS, OS/2, Windows 95 y Windows NT. El UNIX, permiten múltiples tareas y múltiples usuarios.

Otros sistemas operativos multiusuario y multitarea son OS/2, desarrollado inicialmente por Microsoft e IBM, Windows NT y Win95 desarrollados por Microsoft.

El sistema operativo multitarea de Apple se denomina Macintosh OS. El MS−DOS es un Sistema popular entre los usuarios de las computadoras pero solo permite un usuario y una tarea.

Sin duda alguna el tipo de sistema operativo que se desee utilizar va a depender mucho de las actividades a realizar, hoy en día el sistema más popular y comercial es el elaborado por Microsoft, el sistema operativo conocido como Windows en sus diferentes versiones. (Windows 95, Windows 98, Windows XP, Windows Vista, Windows 7, etc.)

Los sistemas operativos han ido evolucionando a medida de las necesidades que se fueron generando, cada sistema operativo tiene un fin determinado que es la de realizar tareas según el objetivo a lograr, dependiendo de lo que necesite el o los usuarios. La mayoría de los sistemas operativos de última generación tienden a, atender un gran número de usuarios, y que los procesos a realizar demoren en un mínimo de tiempo.

3.11 Sistemas Operativos con mayor ataque de virus

¿Todos los virus que existen son compatibles con los diversos tipos de sistemas operativos? Esta pregunta surge cierta confusión entre los usuario ya que si bien es cierto que un virus puede estar presente en la Web por lógica sería que cualquier equipo que accede a la red se infectará, pero no es así, **Un virus informático solo atacará el Sistema Operativo para el que fue desarrollado.**

Los sistemas operativos más atacados por virus informáticos son la línea de Windows de Microsoft, ya que por lógica es mayor el uso de este sistema y por consecuencia se crean más virus y malwares para este sistema.

De los sistemas derivados de Unix como por ejemplo GNU/Linux o Mac OS X de Macintosh, estos han corrido con más suerte de no ser tan atacados debido a que no son tan comerciales, pero cabe señalar que en el pasado, si bien es cierto que no existían virus para estos sistemas, hoy en día se pueden encontrar virus o cualquier malware para estos sistemas, claro que en mayor escala comparado con la implementados para Microsoft.

La ventaja de no tener tantos ataques del sistema operativo Linux es debido a que este sistema es libre, esto significa que no se tiene que pagar ningún tipo de licencia a ninguna empresa desarrolladora de software para el uso de este y otra ventaja que tiene este sistema es que este mismo viene acompañado del código fuente, lo que quiere decir que, cualquier usuario con conocimientos de programación puede manipular el sistema operativo a sus necesidades.

Independientemente de elegir cualquier sistema operativo para el uso del computador, se tienen que tomar las medidas de seguridad adecuadas para poder prevenir cualquier tipo de software malintencionado.

IV
FORMACIÓN DEL USUARIO PARA LA PREVENCIÓN DE POSIBLES ATAQUES INFORMÁTICOS Y SÍNTOMAS DE CONTAGIO DE VIRUS

4.1 Conocimiento Informático del Usuario

En este capítulo se mencionarán ciertas consideraciones que se tiene que tomar en cuenta como usuarios para tener una buena protección y de esta forma poder brindarle a cualquier usuario de la computadora una correcta formación para que a su vez tenga los conocimientos necesarios para poder protegerse de cualquier software dañino.

Existen varios métodos de protección para proteger nuestro ordenador, como lo hemos visto en los capítulos anteriores, como por ejemplo el uso de un antivirus, vacunas, etc., algunas con diferentes formas de operar y todas son herramientas útiles que tienen como objetivo proteger de las posibles amenazas informáticas, ya sea de un virus, de algún troyano o en de algún hacker.

Todas estas herramientas de protección como las que mencionaron en los capítulos anteriores, son el complemento de un buen método de seguridad, que en conjunto nos dan la tranquilidad de tener salvaguardado el equipo de cómputo.

Pero algo sumamente importante y vital para poder combatir con cualquier tipo de malware, es el tener un adecuado y apto conocimiento informático, por ejemplo, como usuarios podemos tener el mejor antivirus en ese momento instalado en nuestro ordenador, podemos tener el mejor firewall, inclusive podemos tener una excelente computadora, pero si no se cuentan con los conocimientos necesarios y competentes de cómo manipular de una manera correcta cada una de las herramientas de protección de nada nos va a servir tenerlas implementadas si nosotros como usuarios no tenemos ni los mínimos conocimientos de su forma de operar.

La finalidad de brindarle al usuario una formación es el evitar los diversos tipos de ataques, ya que con una adecuada formación, se logrará tener la mejor herramienta de protección contra cualquier tipo de virus informático, que es, el conocimiento informático.

Por eso es de suma importancia que como usuarios fomentemos la lectura acerca de los diferentes tipos de amenazas ya que la información acerca de estos tipos de ataques es amplia, se pueden encontrar en libros, periódicos, internet, televisión, foros, conferencias, etc.

4.2 Capacidad de Reconocimiento de diversas Amenazas Informáticas

Es importante que como usuario, tener al menos el mínimo conocimiento acerca de la forma de operar de las incontables amenazas informáticas. Por ejemplo, si nuestro ordenador se llega a ver saboteado por algún hacker algunos de los síntomas de esta daño sería que veamos la pérdida de control de nuestro equipo, se quiere decir con esto que por alguna razón veamos que nuestro equipo este siendo manipulado, si vemos que nuestro mouse se despliega sin que nosotros lo estemos controlando o que nuestro equipo ejecute y abra programas sin que se lo ordenemos, y puede ser que en algunos casos veamos que nuestro equipo se enciende sin razón alguno e inclusive que se desplieguen ventanas y se escriban textos sin nuestra autorización. Entonces si nosotros como usuarios tenemos un mínimo conocimiento acerca de los síntomas generales de los diferentes tipos de virus, podremos tomar las medidas pertinentes para su erradicación.

La capacidad de poder identificar la forma de ataque de cada amenaza informática, es como se podrá combatir cualquier percance en la computadora, es por eso que se recomienda que el usuario siempre este al pendiente de las diferentes amenazas que se suscitan día con día, como se mencionó con anterioridad en los diferentes medios de información, libros, internet, revistas, noticas, etc.

4.3 Discernir los diferentes Tipos de virus

Es importante que como usuarios de la computadora una vez reconocido el tipo de virus informático que se está suscitando, podamos identificar sus características principales y así poder repeler de una manera más fácil el ataque, no es lo mismo tener un gusano alojado en el sistema operativo a tener un virus de sector de arranque, que si bien es importante erradicar los dos, el que tendría mayor

importancia en este caso sería el virus ya que este tipo de virus se encuentra en el sector boot o de arranque ocasionándonos así que el virus se ejecute cada vez que se encienda la computadora, logrando infectarnos numerosos archivos.

Es por eso que se debe tener una buena capacidad de discernir qué tipo de virus es el que está atacando y poder repelerlo de una manera más fácil y sencilla.

4.4 Consideraciones del Sistema Operativo

El siguiente punto es de mucha importancia ya que en el radica la base en la que va a operar la computadora.

Si bien es cierto como ya se mencionó en los capítulos anteriores, existen ciertos tipos de virus para cada sistema operativo, y esto a su vez nos hace más vulnerables a cualquier tipo de virus dependiendo el sistema que estemos manejando. Un usuario que no sabe qué sistema operativo instalar en su ordenador, y este opta por instalar el sistema operativo Linux debido a que este sistema presenta una gran ventaja en contra de los ataques de virus al sistema, con respecto al sistema de Windows, el usuario aparentemente tuvo una decisión correcta ya que es cierto que en la actualidad existen muchos más tipos de ataques al sistema de Windows que al de Linux, pero una vez que el usuario instaló este sistema se da cuenta que no lo sabe usar, que no tiene ni la más mínima idea de cómo se emplea pero a él no le importa tener un escaso conocimiento del sistema ya que él se basó en su única comparación de que sistema operativo es el menos propenso a sufrir un ataque.

La decisión tomada por el usuario fue una medida errónea ya que lejos de beneficiarse, se está haciendo un daño mayor, una observación clara de esto es que si por alguna situación al usuario se le llegara a presentar algún ataque de virus no va a tener el conocimiento adecuado para repelerlo o eliminarlo, ya que como no conoce la forma de operar del sistema que implementó jamás se podrá percatar del ataque del virus, en cambio si hubiera instalado algún sistema que tuviera conocimiento de funcionamiento podría repelerlo de una manera

contundente. Por eso es importante tener el debido conocimiento del sistema operativo que se va a utilizar.

Algunas consideraciones que se podrían tener para el uso o instalación de algún sistema operativo serían:

- Asegurarnos que el software a instalar tenga una procedencia legal, no es lo mismo comprar un sistema operativo en algún punto de venta autorizado a descargarlo de alguna página de internet.
- Permitir una reinstalación rápida del sistema en caso de algún plan de contingencia.
- Tener licencias vigentes del sistema operativo, esto en caso de que lo requiera el sistema.

Un buen sistema operativo no es aquel que nos recomiende otro usuario, o que veamos que tiene mayor publicidad, o mayor demanda, etc., sino es aquel del que tengamos un buen conocimiento del mismo para una operación satisfactoria.

4.5 Consideraciones del Antivirus

Acerca de las consideraciones o características que se deben tener en cuenta para la elección de un buen antivirus, es interminable y muy extenso, y a lo largo de las evaluaciones o aspectos a considerar van a surgir ciertas contradicciones y se vuelve un cuento de nunca a acabar como vulgarmente se dice.

Realmente no existe un antivirus cien por ciento capaz de ser efectivo, pero esto no quiere decir que entre la gran variedad que existe en el ámbito computacional, no exista en comparación, alguno mejor que otro, es por eso conocer qué aspectos se deben tomar en cuenta para la toma de elección de un buen software antivirus.

Existen diferentes maneras en las que se pueden considerar los aspectos a evaluar para un buen antivirus, como por ejemplo podríamos evaluarlos desde un punto comercial o popular, que en este caso analizaríamos a los antivirus más que fueron creadas por grandes empresas del software informático y por lo tanto

tienen un mayor poder de marketing pudiendo así darse a conocer por medio de comerciales, espectaculares, noticias, conferencias, etc.

Otro aspecto a evaluar, sería el funcionamiento del antivirus, con esto se quiere decir en otras palabras, que se observaría a detalle cual es el mejor software haciendo una comparativa de la mejor detección de virus informáticos.

En otro caso más podríamos analizar el mejor antivirus desde un aspecto particular, ¿Qué se quiere decir con esto?, es decir, se analizarían los antivirus a partir de experiencias propias de los diversos usuarios, como dice el escritor De Marcelo, 2000:

“Lo mejor que se puede hacer ante cualquier duda sobre el mejor antivirus que se debe de elegir, es utilizar una copia de evaluación y elegir el que mejor le vaya. Pero observe que un buen antivirus no sólo debe ser de fácil manejo para usted. Una forma válida de es comprobando su capacidad para detectar, no todos, pero por lo menos algún virus nuevo que el antivirus no conozca.” (Marcelo, 2000).

Si bien es un buen punto a evaluar, el que nos da él autor acerca de probar cualquier software antivirus en nuestra computadora, y ver si realmente el software es capaz de detectar algún virus que no se encuentre dentro de su base de datos, esto es un poco complicado, ya que sería mucha pérdida de tiempo el probar todos los antivirus que existen en la actualidad, ya que para iniciar se tendría que recolectar todas las pruebas de evaluación de los antivirus y empezar a probar cada uno de ellos en nuestro ordenador, pero, si en una situación en la que se esté probando algún antivirus, éste mismo no llegase a detectar el virus y por consecuencia perder nuestro sistema operativo o cierto archivo importante, entonces vendría un problema mucho mayor.

Hay infinidad de aspectos que se pueden tener para tomar las mejores consideraciones en la elección de un antivirus, los aspectos que se deben tomar en cuenta para la elección de un buen software antivirus, basados con los diferentes autores como por ejemplo De Marcelo 200, Gómez 2007, así como

también diversos usuarios, artículos publicados y mi experiencia particular, son las siguientes:

- Gran capacidad de detección y de reacción ante un nuevo virus

Es importante que el antivirus sea capaz de detectar con eficacia cualquier tipo de amenaza reciente.

- Actualización

Nuestro antivirus debe tener la capacidad para actualizarse constantemente para combatir las amenazas más recientes, en algunos antivirus existe la modalidad de poder personalizar las actualizaciones, ya sea que el usuario escoja la opción de actualizar por día, o por cada hora, o periódicamente, etc.

- Alertas sobre alguna posible infección

También es importante que el software antivirus tenga la función de emitir alertas para el usuario cuando alguna amenaza se suscité, ya sea por cualquier vía de entrada (Internet, E-mail, Memoria USB, Red, etc.)

- Detección mínima de falsos virus o falsos positivos

Un falso positivo en informática para un antivirus, se refiere a la detección de un archivo como virus (o alguna otra clase de malware) por parte de un antivirus, cuando en realidad no es ningún virus o malware. Estos errores suelen ser pocos, aunque dependiendo de algunos factores (como la heurística, que la heurística son las técnicas que se emplean para conocer o detectar las códigos maliciosos, como los virus, gusanos, troyanos, etc.) puede aumentar la probabilidad de la aparición de estos. (Wikipedia, 2010).

- Rendimiento del antivirus en el ordenador

Si bien es cierto que dependiendo del antivirus es el tamaño del mismo, en algunos casos los softwares requieren mucho espacio en la memoria para poder ejecutarse , aunado a esto cuando estén en ejecución algunos antivirus

llegan a pasmar, trabar o alentar el equipo, ocasionando en casos extremos el reinicio del sistema operativo. Es por eso que es conveniente evaluar el buen rendimiento del antivirus junto con la ejecución de nuestro sistema operativo y demás tareas o aplicaciones que se estén ejecutando.

- Gran capacidad de desinfección

Si por alguna circunstancia nuestro antivirus llegara dejar acceder a un virus a nuestro equipo de cómputo es importante que este mismo tenga la capacidad de eliminarlo para evitar daños mayores.

- Complementos del Antivirus

Es importante que un antivirus no solo detecte los virus informáticos sino que también tenga la capacidad de detectar otro tipo de malwares como lo son troyanos, gusanos, hackers, spams, etc.

- Distintos métodos de detección y análisis

Como se mencionó con anterioridad, existen diversos métodos para la detección de los virus o malwares, es importante que nuestro antivirus tenga diferentes formas de detectarlos ya sea por ejemplo por medio del análisis de escaneo o por medio de algoritmos, entre más variedad de análisis tenga, mejor será nuestra protección.

- Discos de emergencia o rescate

Ciertos antivirus tiene esta función extra, la cual ayuda al usuario, a crear discos de respaldo por cualquier virus que no pueda ser eliminado, esta función lo que hace es crear un copia de nuestro sistema operativo para que en dado caso que algún virus o malware nos llegara a dañar nuestro sistema y no podamos accesar a él, con los discos de rescate podemos reinstalar nuestro sistema operativo tal cual y se encontraba antes del ataque del virus o malware, con la ventaja de que no perderíamos toda nuestra información.

- Soporte Técnico

En algunos casos al momento de adquirir un software antivirus, en la mayoría de los casos por pagar una membresía o una licencia, viene como una característica extra el soporte al usuario, esto quiere decir que en caso de que nuestro antivirus no sea capaz de eliminar cualquier amenaza o en dado caso que nosotros como usuarios no tengamos los conocimientos suficientes para utilizar el antivirus, se brinda una ayuda al usuario, ya sea vía telefónica, asistencia remota o en algunos casos el soporte remoto(se toma el control de la computadora del usuario por medio de una conexión a internet, por una persona capacitada, desde el centro de soporte técnico).

Existen muchas opciones para la elección del antivirus, pero cabe señalar que la decisión final será única y exclusivamente del mismo usuario de la computadora.

La tabla 4.1 muestra un ejemplo de comparación de algunos softwares de antivirus, de tal manera que sea más fácil la elección de alguno.

COMPARACIÓN DE ANTIVIRUS

NOMBRE	VENTAJAS	DESVENTAJAS
Avast Antivirus 6.0	✓ Ocho escudos de protección en tiempo real ✓ Defensa proactiva con el escudo conductual ✓ Módulo de protección para navegación en la Red	✓ El registro gratuito puede resultar molesto ✓ El módulo de reputación carece de web propia ✓ Ventana de gran tamaño
AVG Antivirus 2012	✓ Agradable interfaz gráfica ✓ Escáner de enlaces (Link Scanner) ✓ Protección en Redes Sociales ✓ Gadget para el escritorio	✓ La optimización de análisis es muy lenta

Kaspersky Antivirus 2012	✓ Fácil uso con menús claros ✓ Análisis rápido y completos ✓ Perfil para juegos ✓ Disco de rescate ✓ Revisión de enlaces URL	✓ Actualización de formas un poco lenta ✓ Elevado consumo de recursos
ESET Nod32 Antivirus 5.0	✓ Heurística Avanzada ✓ Análisis muy rápidos ✓ Consumo de memoria reducido ✓ Protección mediante contraseñas ✓ Inspector de sistema y actividad	✓ Ninguno destacable
Norton Antivirus 2012	✓ Detección de malware de gran nivel ✓ Entré los más rápidos de la categoría ✓ Instalación rápida ✓ Modo silencioso ✓ Widget para el escritorio	✓ Mapamundi vistoso pero poco útil ✓ El diagnóstico de rendimiento es lento ✓ Poca información durante el análisis

TABLA 4.1 (Softonic, 2011)

4.6 Consideraciones de la Red

Como ya se ha mencionado con anterioridad, una de las formas de contagio de un virus informático o cualquier tipo de malware es por la vía del Internet, es por eso que en este punto, se mencionarán las consideraciones que se deben de tener para evitar cualquier tipo de dichas amenazas.

Es importante que el usuario tenga conciencia acerca del gran impacto que tiene el Internet en estos días, si bien es cierto que este mismo trae grandes beneficios, como por ejemplo el envío de correos electrónicas, transacciones bancarias, información detallada, etc., también puede representar una gran amenaza si no se toman las medidas correctas para su funcionamiento, ya que gracias a las miles

de redes que existen en el mundo informático, los equipo son muy susceptibles a un contagio de un virus.

Si en alguna computadora se llegase a conectar a Internet, la cual no nos hemos percatado de que se encuentra infectada por un virus, y una vez que estamos conectados a Internet abrimos alguna aplicación que implique la conexión a la red, estaremos propagando ese virus a cientos y cientos de computadoras, como lo suele ser en algunos casos que algún usuario ejecute la aplicación de Messenger y que el virus que se encuentre en esa computadora, empieza a desplegar avisos a los contactos que se tengan agregados, de tal manera que los demás usuarios abran cierto link o acepten alguna descarga que aparentemente es mandada por el usuario que ellos conocen y de esa manera el virus empiece a propagarse.

Otro aspecto muy importante a considerar es la precaución para navegar que los usuarios deben de tener, se ha dado el caso que muchos usuarios empiezan a navegar por la red, visitando miles y miles de páginas de Internet y cuando menos se lo esperan su equipo ya ha sido infectado por algún malware, esto debido a que muchas veces no se dan cuenta que las páginas que vistan son creadas por hackers o simplemente se encuentran infectadas y al momento de accesar a ellas surge el contagio. O también puede darse el caso que al momento de visitar estas páginas pidan al usuario instalar ciertos complementos aparentemente para poder ver algún contenido de la página y esto ocasiona que se instale algún virus o malware y si aunado a todos estos ejemplos agregamos que nuestra computadora una vez que se encuentra ya infectada le agregamos que se encuentra dentro de una red de trabajo, pues el daño ya es mayor porque no solo corremos el riesgo de que dañe nuestro equipo de cómputo sino que se dañarían todos los equipo que se encuentren dentro de la red. A continuación se mencionan algunos puntos importantes que se deben de tomar en cuenta en una red para la protección contra cualquier malware.

- **Firewall**

Es importante tenerlo instalado en la computadora ya que ayuda a filtrar contenidos y puntos de acceso, nos da la seguridad de que otra persona no autorizada tenga acceso desde otro equipo al nuestro.

- **Controlar y Monitorear el acceso a Internet**

Esta consideración nos permite restringir el acceso a ciertas páginas que pueden resultar malignas para nuestra computadora.

- **Filtrados de Firewall de Red**

Esta consideración sería el de eliminar todos aquellos programas que compartan datos a través de Internet, como lo pueden ser los P2P, que son los softwares que se usan para descargar música, aplicaciones sin licencias, videos, etc., un ejemplo de los softwares que utilizan el P2P son Ares, LimeWire, etc.

- **Jerarquización de Usuarios**

Este punto nos ayuda a restringir a ciertos usuarios de la red de tal manera que puede prevenirse una amenaza. Por ejemplo si en una empresa que tiene su red de trabajo, se encuentra un director de sistemas, un asistente y un trabajador externo, los permisos para la persona externa a la empresa no van a ser iguales a los del director, de esta manera estaremos previniendo un mal uso que pueda llegar a tener en la red.

- **Centralizar Datos**

En esta medida lo que hace es que se disponen de detectores de virus, como por ejemplo algún antivirus y se ejecutan durante el tiempo inactivo de las máquinas que se encuentren en la red, en busca de alguna amenaza.

4.7 Acciones Preventivas

Conocer los mecanismos de cualquier tipo de virus informático para su propagación y la forma en que toma el control de nuestro equipo de cómputo. Existe una ley acerca del comportamiento de los virus informáticos y es que para que puedan reproducirse es necesario que el programa que lo tiene lo ejecute. Esta ley nos dice en pocas palabras que para que un virus informático tome el control de nuestra computadora es necesario que nosotros como usuarios ejecutemos el programa que sirve como huésped del virus, sino no habría forma de contagiar nuestro equipo.

Los virus utilizan una forma de camuflaje lo cual se hace más difícil poder detectar algún programa que se encuentre como huésped de cualquier virus, que si bien es cierto un software antivirus nos puede ayudar a detectar algún programa infectado cabe señalar que este mismo no nos da el cien por ciento de garantía de que detecté todas las amenazas que se lleguen a tener en nuestra computadora, es por eso que los usuarios tomemos deben tomar acciones preventivas para minimizar el riesgo de contagio.

1) **Primera acción** preventiva viable para evitar el contagio de cualquier virus es el no instalar copias piratas en nuestro ordenador, ya que muchas veces el instalar programas de los cuales desconocemos su procedencia o en algunos casos también no se sabe quién es el autor del mismo, esto nos está haciendo más propensos a tener un virus o malware en nuestro equipo.

Claro que si uno como usuario conociendo todos los riesgos que con lleva instalar algún software pirata se decide tomar los riesgos al instalar cualquier programa de estos, entonces es recomendable contar con los métodos de protección correspondientes que podrían ayudar en dado caso de un posible infección a proteger el equipo de cómputo, como lo pueden ser el uso de un antivirus o de vacunas.

2) **Segunda acción** de prevención es el tener la responsabilidad de darle un uso correcto a nuestro equipo de cómputo, con esto se quiere decir que el usuario es responsable en el uso correcto de la computadora, pero si somos de aquellos usuarios que suelen prestar sus computadoras a cualquier persona que conozcamos sin tomar las medidas pertinentes, le estaremos ocasionando un daño a la computadora, ya que muchas veces desconocemos el uso que le dan aquellas personas a nuestra computadora, no sabemos si la usen para instalarles programas piratas, si se use para descargar algo de la red o en caso dado que realmente se le dé un uso correcto al equipo pero que la persona que la está utilizando no tenga un apto conocimiento informático y por consiguiente llegue a mover archivos importantes del sistema operativo, elimine documentos importantes, acepte la ayuda de cualquier usuario que tengas las intenciones de dañar nuestra computadora, etc.
3) **Tercera acción** preventiva consiste en el aislamiento durante el ataque. En la empresa IBM se dice que cuando se detecta un ataque en la red, "desconectan la clavija". Eso no significa que estén a salvo. Si un virus se ha esparcido durante seis meses y causa daño hoy, desconectar la clavija de la red no ayuda. Por otra parte, si el ataque es tenue y lento, desconectar la clavija podría ayudar.

   En la mayoría de las grandes organizaciones actuales, desconectarse de la red global resultaría desastroso, pues no tendrían acceso a los servicios, de modo que hay una relación entre utilidad y seguridad.

Como podemos ver existen varias acciones preventivas que los usuarios de la computadora pueden emplear para su protección, pero una acción preventiva ideal para la protección ante cualquier virus informático o malware es una combinación adecuada de prudencia (en la introducción de programas) y herramientas de protección contra los virus (antivirus, vacunas, respaldos, etc.) para poder de cierta forma garantizar la relativa seguridad y protección del ordenador.

4.8 Síntomas de Contagio

Generalmente existen diversos tipos de síntomas al infectarse de un virus informático, que si bien es cierto algunos de estos síntomas son importantes analizarlos ya que gracias a ellos podremos identificar en algunos casos el tipo de virus que nos está atacando y de esa manera poder combatirlo de una mejor manera. Pero en rasgos más generales muchos usuarios se hacen la pregunta anunciada, ¿Cómo identifico o qué síntomas debe tener mi equipo de cómputo para saber si está infectada por algún virus informáticos?, esta pregunta es muy común entre los millones de usuario que día a día utilizan su ordenador, a continuación se identificarán algunos síntomas de contagio más comunes.

Existe una forma muy usual de mencionar diversos tipos de síntomas debido al contagio de un virus informático entre ellos podemos encontrar por ejemplo, **retardos** que no se presentaban con anterioridad ante la ejecución de un programa, con esto se quiere decir que si normalmente nosotros como usuarios por ejemplo ejecutamos algún programa como lo puede ser algún paquetería para editar texto y al momento de cargarlo o ejecutarlo tarda más de lo inusual y que esta anomalía no solamente la haga con ese programa sino que con diferentes software puede ser un posible síntoma de contagio de virus.

Otro ejemplo de síntoma, es el **cambio de longitud** de los programas instalados en nuestro equipo de cómputo, en pocas palabras, si nosotros como usuario tenemos instalado por ejemplo un software que al momento en que nosotros lo instalamos nos percatamos de que ocupaba un tamaño de 5 Megabytes y con el paso del tiempo este mismo incrementó su capacidad a por ejemplo 25 Megabytes sin realizar ninguna actualización o instalarle algún complemento, este es también un posible síntoma de contagio de virus.

Existen muchos más, pero estos mismos síntomas tienen ciertas diferencias entre cada uno de ellos, es por eso que una forma más sencilla de identificarlos esto es haciendo una clasificación de los mismos, estos son los Síntomas Estáticos y los Síntomas Dinámicos.

4.9 Síntomas Estáticos

A continuación se describen unos ejemplos de los Síntomas Estáticos:

- Desaparecen archivos del usuario que por lo regular un virus suele borrar y también estos mismos cambian el nombre del volumen del disco duro.
- Aparecen nuevos archivos cuya procedencia no tiene explicación.
- Actualizaciones de los archivos de programas sin ninguna causa.
- Se modifican archivos a consecuencia del virus

4.10 Síntomas Dinámicos

A continuación se describen unos ejemplos de los Síntomas Dinámicos:

- En la pantalla aparecen mensajes o imágenes que anteriormente no aparecían.
- Programas que durante un largo periodo funcionaban sin problemas, repentinamente dejan de hacerlo.
- Cualquier programa que se ejecute responde con mayor lentitud, ya que primero corre el programa de virus.
- Se incrementa sin ninguna explicación el espacio usado en la memoria.

Como se ha observado existen varios ejemplos de síntomas por contagio de un posible virus, pero es importante mencionar los usuarios de un ordenador deben de estar siempre al pendiente de cualquier anomalía o síntoma que consideremos relevante o poco inusual, ya que si el computador llegase a estar infectado y por consiguiente empieza a presentar dichos síntomas y nosotros hacemos caso omiso, podemos estarle ocasionando un daño importante a nuestra computadora, que con el paso del tiempo puede irse incrementando. Es por eso que una vez que identifiquemos los síntomas actuemos de manera oportuna y eficaz para evitar posibles daños críticos.

V

ACCIONES Y PLAN DE CONTINGENCIA PARA ATAQUES INFORMÁTICOS

Como se ha mencionado con anterioridad es importante tener medidas o acciones de prevención para poder proteger a un ordenador de cualquier ataque de un virus informático, pero aun cuando se tomen las medidas de prevención adecuadas siempre existe una posibilidad de riesgo de contagio, es por eso que en este capítulo no solo se mencionaran las medidas de prevención, sino que también se mostrará un plan de contingencia en caso de adquirir en nuestro ordenador un ataque de virus informático, de esta manera podremos eliminar o desinfectar nuestro ordenador para que su funcionamiento sea el adecuado para que le sea posible realizar de manera satisfactoria las tareas que les sean asignadas.

5.1 Solución para futuros ataques de virus

En los capítulos anteriores se han visto diferentes formas de protección en contra de los virus informáticos, gusanos, troyanos, etc., como el uso de un software antivirus, el uso del firewall, el empleo de vacunas, que de cierta manera dan al usuario una tranquilidad aparente, esto debido a que como se ha mencionado con anterioridad por más que se empleen las medidas de protección correctas para la protección de un ordenador siempre existen causas internas o externas que pueden ser propicias para la infección del mismo.

Como lo menciona el autor Nombela, 1991: “Desafortunadamente, uno nunca sabe cómo es posible que al final haya aparecido ese maldito virus en nuestro ordenador, pese a todas las medidas de protección que hemos tomado” (Nombela *et al*., 1991).

O como también lo menciona en esta reseña el Doctor Spafford Eugene H. y profesor en Ciencias de la Computación: “El único sistema realmente seguro es aquel que está apagado, guardado en una caja fuerte de Titanio, encerrado en un bunker de concreto, rodeado por gas venenoso y cuidado por guardias muy armados y muy bien pagados. Aun así no apostaría mi vida por él” (1999).

Es cierto que una manera de prevenirse de futuras amenazas de virus informáticos es el tener los antecedentes por los cuales se propició la infección del ordenador, por ejemplo, si nosotros como usuarios cometimos el error de instalar

un software sin licencia del cual desconocemos su procedencia, o introducimos una memoria usb infectada sin antes analizarla con un software antivirus y a consecuencia de ello el ordenador se infectó, entonces tendremos los puntos a mejorar en los cuales no se puso la adecuada atención y de esa manera no volver a cometer los mismos errores.

Pero también existen otras medidas de solución para la prevención de futuros ataques de virus, estas medidas de prevención se pueden clasificar en medidas primarias y secundarias, estas medidas tiene como objetivo prevenir de posibles futuras infecciones de virus informáticos y de esta manera poder minimizar la pérdida de información de nuestro ordenador.

5.2 Medidas de Prevención Primaria

A continuación se describen algunos ejemplos:

- ✓ Prepare un disco de arranque "limpio" (verificado contra virus) y protegido contra escritura.
- ✓ No utilice Memorias o CD que no sean suyos sin revisarlos antes.
- ✓ Revise sus discos o dispositivos de almacenamiento si se utilizaron en otra computadora que no sea la suya, sobre todo si los utilizaron en máquinas conectadas a red.
- ✓ Instale al menos un programa antivirus, esté conectado o no a una red.
- ✓ Evite la copia ilegal de programas, juegos y utilitarios.
- ✓ Mantenga activado siempre el centinela (TSR) del programa antivirus. Si tiene más de un programa antivirus configúrelo para que trabaje SÓLO UNO de los centinelas.
- ✓ Revise todo su sistema si presenta un funcionamiento anormal, no acostumbrado.
- ✓ Chequee periódicamente todo su sistema (una vez a la semana), independientemente del centinela del antivirus.

5.3 Medidas de Prevención Secundaria

A continuación se describen algunos ejemplos:

- ✓ No ejecute ningún programa, excepto un antivirus, hasta que descontamine su computadora.
- ✓ Aun cuando descontamine sus aplicaciones, y estas funcionen adecuadamente, lo ideal es realizar su reinstalación.
- ✓ Arranque su computadora con un disco de arranque, verificado contra virus y protegido contra escritura.
- ✓ Crear periódicamente un disco de respaldo para no perder la información que considere importante. (El tiempo establecido para elaborar el disco de respaldo varía dependiendo de cada usuario y de las actividades que realice nuestro operador, no es la misma importancia el crear el respaldo de un ordenador que sirve como servidor de La Bolsa Mexicana de Valores, al de un ordenador de uso familiar).

5.4 Detección de virus informáticos

Como se ha visto en los capítulos anteriores existen varios programas o softwares, los cuales se encargan de prevenir, detectar y eliminar cualquier software maliciosos, pero también vimos que independientemente del software que se haya instalado en nuestro ordenador para su protección, hemos visto que no todos ellos tiene la certeza de brindarnos un seguridad plena, es por eso que es importante que nosotros como usuarios tengamos la capacidad de detectar ciertas anomalías que son propiciadas por algún virus o malware.

La forma más evidente de detección es cuando el mecanismo destructor del virus ya se ha disparado, realmente no hace falta ser un genio para deducir que tenemos un virus informático cuando empiezan a aparecer mensajes desconocidos en el monitor, o que surgen pelotitas brincando en toda la pantalla o en su defecto que nuestra impresora imprima datos sin ningún motivo o razón.

Existen, sin embargo, formas de detectar la presencia de virus antes de que la acción destructora comience, durante la fase en que el virus está aún reproduciéndose. La propia actividad reproductora y los mecanismos de enmascaramiento del virus dejan pistas que pueden ser en ocasiones fácilmente detectables. (Nombela *et al*., 1991).

En este proceso podemos encontrar diferentes utilidades para su detección, a continuación se explicarán algunas de ellas:

- **Antivirus**

Los softwares Antivirus son una buena ayuda para la detección de posibles virus informáticos ya que permiten identificarlos al momento de realizar un escaneo periódicamente del sistema. De esta forma, un comparador de paridad nos informará si he producido una modificación a los ficheros analizados sin el consentimiento del usuario. Por ejemplo, un programa vacuna nos sirve de muy poca ayuda al tratar de impedir las actividades de reproducción de un virus, por ejemplo una serie de disparos injustificados o de la activación de la vacuna de una manera inaudita, es un indicio casi seguro de que en nuestro equipo de cómputo está infectado por un virus.

- **Retardo del funcionamiento del ordenador**

Otro indicio que podemos comentar, acerca de la detección de un posible virus en nuestro equipo de cómputo, es el retardo o lentitud de trabajo del mismo. Esto se debe a que la mayoría de los virus deja su código residente en la memoria al ejecutarse un programa infectado, por ejemplo si nosotros como usuarios notamos que al abrir ciertos programas que normalmente no se retrasan o demoran al usarlos y observamos que de un tiempo a la fecha realiza este retraso es casi seguro de que podemos tener infectada nuestra computadora.

Una prueba que podemos realizar nosotros como usuarios es por ejemplo, una vez que hayamos detectado el programa que presenta una lentitud considerable, entonces procedemos a realizar lo siguiente, apagamos el ordenador y lo iniciamos como normalmente lo hacemos, después procedemos a ejecutar el programa que presenta la falla y si observamos que en un principio el programa está en un funcionamiento óptimo pero después de unos minutos sin razón alguno se pasma, se traba o alenta puede ser que este infectado por virus.

- **Sectores Ocultos**

Algunos virus contaminadores del boot record (es el primer sector de almacenamiento de datos, en este caso del disco duro), utilizan técnicas de ocultación para de sectores para guardar su código y protegerlo del sistema operativo. De esta forma los virus modifican los archivos de ficheros, de tal manera que en algunos casos ahí mismo ocultan o guardan su código haciendo de esta forma que el tamaño o el espacio de los ficheros aumente. Para poder detectar este hecho podemos utilizar la utilidad “CHKDSK” ejecutándola en el modo MS-DOS de nuestro sistema operativo de Windows, que nos avisará de cualquier discrepancia entre el tamaño real del fichero y el tamaño que se detectó, si existe dicha diferencia entre el tamaño es casi seguro que un virus se ha introducido.

- **Otros indicios**

En general cualquier funcionamiento anormal del ordenador puede ser indicio de la existencia de un virus informático, pero existen dos síntomas que resultan sospechosos que son: los accesos injustificados al disco duro y los mensajes inoportunos del sistema operativo.

Acerca del acceso al disco duro podemos observar que algunos programas realizan este procedimiento intentando efectuar alguna modificación en los archivos de los ficheros contenidos en ese disco, pero ese síntoma debe ser

tratado con cuidado ya que muchos programas acceden de forma constante al disco duro por ejemplo para llevar un registro de las actividades o realizar copias de seguridad, por eso es importante prestar mucha atención a este síntoma de un posible contagio de virus.

El segundo indicio acerca de los mensajes inoportunos es algo fácil de detectar por así decirlo, ya que la característica de este síntoma como su nombre los dice, es la aparición de mensajes raros en el sistema sin que existe una explicación lógica de los mismos, por ejemplo en algunos casos cuando el virus ya se encuentra en el ordenador, el creador del mismo envía o despliega mensajes en el monitor de tal manera que logré aterrorizar al usuario.

5.5 Eliminación de virus informáticos

Si bien es cierto que existen diversas maneras de poder eliminar o erradicar un virus informático, como la mayoría de los usuarios informáticos conocen la manera más común o popular de erradicarlos es el uso de un software antivirus, pero cabe mencionar que esta no es la única manera para poder combatirlos, en los siguientes incisos se explicarán las diferentes formas y a su vez su funcionamiento para la eliminación de los virus.

a) Eliminación por medio de Detectores Antibomba

Esta función lo que hace es que explora los archivos buscando rutinas peligrosas, por ejemplo órdenes de borrado de archivos. Anteriormente era los más usados pero llegaron a tener una época de crisis pero al parecer vuelven a retornar en estos tiempos. El único inconveniente para el uso de estos detectores es que, para poder operarlos de una manera adecuado, es necesario tener buenos conocimientos tanto de hardware como de software.

b) Eliminación por medio de Antivurs

Un virus puede dejar rastros de su actividad, y ahí es donde entra en escena esta tipo de softwares, en general son bastante eficaces, y su uso no requiere

de un extenso conocimiento informático, es por eso que por lo regular son los más usados.

c) Detector de Virus Concretos

Buscan un número de determinado de virus conocido que llevan en su base de datos por medio de lo que se le conoce como “Cadenas de detección o Firma”, una vez que el virus queda identificado se realiza una eliminación.

Otra versión de este tipo de detectores sería la vacuna concreta contra un virus determinado, ya no se hacen mucho, salvo que el virus sea nuevo y se necesite un borrado con urgencia.

d) Detector Genérico

Estos se encargan de vigilar o monitorear el tamaño de los archivos ejecutables. El problema es de que en la actualidad hay varios virus que pueden aumentar el tamaño de un archivo sin que se note dicha modificación por esa razón su eficiencia se ha visto reducida.

e) Detectores de Macros

Estos son especiales para los macrovirus. Un Macrovirus es un virus programado en lenguaje de "macro" de una aplicación, que infecta a los archivos de información generados por dicha aplicación para generar copias de sí mismo, tomar el control del sistema y generar algún tipo de daño. En la actualidad la mayoría de los macrovirus están escritos con el lenguaje de programación de macros del Microsoft Office para Windows (recordemos que el Word Basic es un subconjunto del lenguaje Visual Basic) y pueden ser desarrollados para cualquiera de sus aplicaciones (Word, Excel y Access). (Anónimo. *Macrovirus*, [Web en línea])

f) Vacunas de Desastre

Es una herramienta que sirve en el caso de que se ha producido un destrozo de alguna parte del disco por culpa de la intrusión de un virus informático, estas vacunas restauran el buen funcionamiento del sistema, pero atención, se han perdido datos estos no se podrán recuperar, en este caso aquí es conveniente tener copias de seguridad para recuperar esa pérdida de información, en algunos casos este tipo de programas vienen incluidos en los paquetes de los antivirus.

g) Vacunas de Desinfección

Estas eliminan un tipo determinado de virus en un tipo determinado de archivo. Estas vacunas se quedan antiguas o anticuadas ya que aparecen constantemente nuevo virus y nuevas mutaciones. (Marcelo, 2000).

5.6 Acción en caso de la imposibilidad de la eliminación de virus

Una vez que nuestro ordenador se encuentra infectado por un virus, es determinante realizar una acción rápida para la eliminación de este. Al retrasarse la erradicación, puede propagarse la infección hasta el punto, que incluso llegue a ser imposible eliminar los virus sin poder evitar la pérdida de datos. Es probable que algunos usuarios, aun sabiendo que en su computadora se encuentra infectada por un virus, continúen utilizándola, mientras el virus se multiplica internamente. En estos casos algunos usuarios no captan la severidad del problema en que se encuentra o en algunos situaciones piense que el problema desaparecerá en algún momento, pero lo que no analizan es que esos valiosos documentos en que continúa trabajando tal vez se convertirán en algo irrecuperable si los virus logran atraparlo. Es recomendable en la mayoría de los casos ejecutar lo más pronto posible un programa antivirus o un par de ellos, que encuentre los archivos con virus y los arregle si es posible. De lo contrario, los deberá eliminar y si se trata de archivos o programas importantes, deben

sustituirse luego por sus originales (que debería tener como respaldo) para terminar el proceso de reparación.

Pero existen ciertos casos en los cuales una vez que el ordenador se encuentra infectado por un virus y este a su vez no es atendido correctamente, se corre también el riesgo de no solo contraer un solo virus informático sino más de uno o en dado caso no solo puede estar contagiado por un virus sino también por algún otro malware como lo es un troyano, un gusano, inclusive por un hacker. En estas circunstancias es muy difícil poder eliminar todos los malwares que se encuentren en el ordenador, que si bien es cierto que existe la remota posibilidad de hacerlo es casi nula poder recuperarse de tantos ataques, ya que en estas circunstancias se pierde por completo el control del equipo.

La medida drástica para efectiva para una eliminación segura de un virus informático o cualquier malware en caso de no poder erradicarlo es el “formateo” de nuestro ordenador, esta actividad lo que implica es borrar todo lo que está almacenado en el disco duro donde está instalado nuestro sistema operativo, es decir que se borrará toda la información junto con el sistema operativo y de esta manera por obviedad se eliminará cualquier tipo de virus o malware que se encuentre en el ordenador.

Si bien es cierto que esta medida es cien por ciento segura para la eliminación de cualquier virus informático o malware, cabe señalar que no cualquier usuario puede realizarla ya que como su descripción lo dice, esto implica un borrado completo de todo el sistema, es decir, que no solo se borran archivos o programas sino que también se borran los drivers o controladores del equipo de cómputo “Un driver o controlador, es un programa que controla un dispositivo. Cada dispositivo, ya sea una impresora, un teclado, una tarjeta de video, tarjeta de sonido, etc., debe tener un programa controlador. Un controlador actúa como un traductor entre el dispositivo y los programas que utilizan el dispositivo.” (Masadelante.com. *¿Qué significa un driver?*, [Web en línea]. 1999-2011), ocasionando que no podamos utilizar de manera adecuado los componentes de la computadora, pero no solo es

necesario contar con los drivers adecuados para la reinstalación sino que también es necesario contar con los programas y con sus respectivas licencias para poder instalarlos, si en estos casos se cuenta con un disco de respaldo nos estaríamos ahorrando mucho tiempo para reinstalar adecuadamente la computadora pero es cierto que al momento de tener un disco de respaldo no quiere decir que los programas que teníamos instalados en nuestro ordenador aparezcan por arte de magia, ya que ciertos softwares tienen sus respectivas licencias para poder instalarlos.

Aunado a estos requisitos que necesitamos para poder formatear nuestro ordenador, un punto importante y si no el más relevante, es el tener el sistema operativo para poder instalarlo en nuestro ordenador, por ejemplo si nosotros como usuarios tenemos discos de respaldo de nuestros archivos, tenemos todos los programas junto con sus licencias pero no tenemos el sistema operativo con su respectiva licencia no podremos realizar el formateo del equipo, por el lado contrario, si tenemos el sistema operativo a instalar con su respectiva licencia pero por ejemplo no tenemos los programas o los drivers del ordenador, aun así podremos realizar el formateo del equipo, siendo que después de haber realizado el formateo e instalado el sistema operativo es posible conseguir los drivers o en su defecto los programas que se deseen instalar.

CONCLUSIÓNES

En la presente tesis se han expuesto diferentes medidas de protección contra cualquier software malicioso que se presente en cualquier ordenador o computadora, se han sugerido diversos métodos que como usuarios de los ordenadores podemos llevar a cabo para una adecuada seguridad de la información digital.

Se analiza y se da a conocer la magnitud que con lleva el no tener un adecuado conocimiento de los diferentes métodos o herramientas que se pueden implementar en una computadora, para así salvaguardar nuestra información.

Se denotan los complementos y las medidas de prevención necesarias para repeler cualquier tipo de software malicioso, se muestra que no basta con fomentar una buena educación informática en el usuario de cualquier ordenador, tampoco basta tomar todas las medidas o herramientas adecuadas para la caución de cualquier ataque informático, porque por más que se tomen dichas acciones siempre existe una amenaza latente, es por eso que en la presente tesis también se sugiere e implementa un plan de contingencia con el cual nos brinda las acciones para llevar a cabo la erradicación de cualquier malware.

La aportación a la Hipótesis presentada de saber si realmente existe un método de protección capaz de ser cien por ciento confiable, eficiente y no vulnerable ante cualquier amenaza informática serían las siguientes conclusiones.

1. Actualmente y en tiempos futuros, no va a existir un medio que sea cien por ciento confiable, debido a que hoy en día las amenazas informáticas constantemente están evolucionando, ya que cuando surge una vacuna o un método de protección para cualquier tipo de amenaza, ya está nuevamente en la lista de espera otra vacuna necesaria para un nuevo malware.

2. No existe un Antivirus cien por ciento invulnerable ante las amenazas informáticas. (Se comparten y mencionan dos referencias de autores de libros e investigadores que se desarrollan en el ámbito informático los cuáles coinciden con lo anteriormente concluido.)

   Doctor Spafford Eugene H. y profesor en Ciencias de la Computación: "El único sistema realmente seguro es aquel que está apagado, guardado en una caja fuerte de Titanio, encerrado en un bunker de concreto, rodeado por gas venenoso y cuidado por guardias muy armados y muy bien pagados. Aun así no apostaría mi vida por él" (1999).

   Bruce Schneier, estadounidense, Criptógrafo, experto en Seguridad Informática y Escritor: "Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología"

3. Fomentar la educación informática del usuario para minimizar cualquier contagio o infección.

4. Contar con un plan de contingencia que el usuario pueda implementar en la detección y eliminación de cualquier tipo de virus informático.

En conjunto los cuatro puntos anteriores forman lo que se puede denominar una cultura informática que permite al usuario salvaguardar la información y protección del equipo de cómputo personal o de cualquier organización.

BIBLIOGRAFÍA

Fuentes Citadas (Libros)

- Álvarez Marañón, Gonzalo, *Cómo protegernos de los peligros de Internet.* Editorial Los Libros de la Catarata, 2009.
- Cohen, Frederick B, *Curso abreviado de virus en computación.* Editorial Limusa, México, 1998.
- Cohen, Frederick B., *A shorth course on computer viruses.* Editorial J. Wiley, New York, 1994.
- Cortes, Pedro Luis, *Virus: Manual de referencia.* Editorial Ventura, México, 1994.
- Dhanjin, N; B. Rios y B. Hardin, *La nueva generación Hacker.* Editorial Anaya Multimedia, Madrid, 2010.
- Fernández F., R. y M. Ontiveros, *Historias de la historia del cómputo en México.* Editorial Servicio de Consultoría de Valor Agregado, 2008.
- Ferreyra Cortés, Gonzalo, *Virus en las Computadoras.* Editorial Computec, México, 1995.
- Gómez Vieites, Álvaro, *Enciclopedia de la Seguridad Informática.* Editorial Alfaomega Grupo Editor, México D.F., Mayo 2007.
- Hoffman, Lance J., *Rogue programs: Viruses, worms, and trojan horses.* Editorial Van Nostrand Reinhold, New York, 1990.
- Levin, Richard, *Virus informáticos: Tipos, protección, diagnosis, soluciones.* Editorial McGraw-Hill, México, 1992.
- Marcelo Rodao, Jesús de, *Guía de campo de los virus informáticos.* Editorial Alfaomega, México, 1997.
- Marcelo Rodao, Jesús de, *Piratas cibernéticos: cyberwars, seguridad informática e Internet.* Editorial Ra-Ma, España Madrid, 2001.
- Marcelo Rodao, Jesús de, *Virus de Sistemas Informáticos e Internet.* Editorial Alfaomega Grupo Editor, México D.F., Octubre 2000.

- Mur A; P. Nieto y J. Molina, *Virus Informáticos.* Editorial Anaya Multimedia, Madrid, 1990.
- Nombela J; L. Pino y J. Pino, *Virus Informático.* Editorial Paraninfo, España Madrid, 1991.
- Oriyano, S., P. y M. Gregg, *Hacker techniques, tools, and incident handling.* Editorial Jones and Bartlett, 2011.
- Rodríguez Cárdenas, Mario, *Saque virus y rescate archivos perdidos: Como echar fuera un virus de su computadora teclazo por teclazo y como rescatar la informacion perdiada que pensaba irrecuperable.* Editorial Rocar, México, 1990.
- Seoane, José Alberto, *Acoso digital: prevención y antídotos.* Editorial Macchi, Argentina Buenos Aires, 2001.
- Walker, Andy, *Manual imprescindible de seguridad, spam, spyreware y virus.* Editorial Anaya Multimedia, España Madrid, 2006.

Fuentes Citadas (Páginas Web)

- Alegsa. "Características de los virus informáticos", [Web en línea]. 1998-2011, [05 de Septiembre de 2011]. Disponible en la Web: http://www.alegsa.com.ar/Notas/270.php
- Anónimo. "¿Qué es un antivirus?", [Web en línea]. 2001-2011, [27 de Septiembre de 2011]. Disponible en la Web: http://www.sitiosargentina.com.ar/webmaster/cursos%20y%20tutoriales/que_es_un_antivirus.htm
- Anónimo. "¿Qué es un Sistema Operativo?", [Web en línea]. 2009-2011, [15 de Agosto de 2011]. Disponible en la Web: http://www.masadelante.com/faqs/sistema-operativo0
- Anónimo. "¿Qué es un VIRUS Informático?", [Web en línea]. 2011, [18 de Agosto de 2011]. Disponible en la Web: http://www.slideshare.net/neto.15chavez/que-es-un-virus-informatico-1142698

- Anónimo. “Macrovirus”, [Web en línea]. [16 de Noviembre de 2011]. Disponible en la Web:
- EURAM. “¿Qué es un Sistema Operativo?”, [Web en línea]. (2000), [21 de Octubre de 2011]. Disponible en la Web: http://www.euram.com.ni/pverdes/verdes_informatica/informatica_al_dia/que_es_un_so_144.htm http://www.oni.escuelas.edu.ar/2003/buenos_aires/73/Macrovirus.htm
- Fernández, Borja. “ Frases célebres de Seguridad Informática”, [Web en línea], [15 de Diciembre de 2011]. Disponible en la Web: http://beartigo.wordpress.com/2008/05/12/frases-celebres-de-seguridad-informatica/
- Manson, Marcelo. “Estudio sobre virus informáticos”, [Web en línea]. 2011, [06 de Septiembre de 2011]. Disponible en la Web: http://www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml
- Masadelante.com. “¿Qué es un Driver?”, [Web en línea]. (1999-2011), [16 de Noviembre de 2011]. Disponible en la Web: http://www.masadelante.com/faqs/driver
- Masadelante.com. “¿Qué es un Sistema Operativo?”, [Web en línea]. (1999-2011), [21 de Octubre de 2011]. Disponible en la Web: http://www.masadelante.com/faqs/sistema-operativo
- Microsoft Corporation. “¿Qué es una firma digital?”, [Web en línea]. (2011), [28 de Octubre de 2011]. Disponible en la Web: http://windows.microsoft.com/es-ES/windows-vista/What-is-a-digital-signature
- Museo de la Informática y Computación Aplicada. “Historia”, [Web en línea]. (2003-2010), [17 de Mayo de 2012]. Disponible en la Web: http://www.tecnotopia.com.mx/logitronica/virhistoria.htm
- Norton. “Los diez virus informáticos más peligrosos de la historia”, [Web en línea]. (03 de Enero de 2011), [07 de Septiembre de 2011]. Disponible en la Web: http://www.nortonfanclub.com/?p=278

- Seguridad Informática. “Ciclo de Vida de un Virus”, [Web en línea]. (2004-2011), [01 de Septiembre de 2011]. Disponible en la Web: http://seguinfo.wordpress.com/2006/04/10/ciclo-de-vida-de-un-virus-2/
- Softonic International S.L. “Antivirus”, [Web en línea]. (1997-2011), [06 de Octubre de 2011]. Disponible en la Web: http://www.softonic.com/windows/antivirus-genericos:programas
- Universidad Católica Nuestra Sra. de la Asunción. “Virus Informáticos”, [Web en línea]. (Junio de 2001), [09 de Noviembre de 2011]. Disponible en la Web: http://www.dei.uc.edu.py/tai2001/virus/index.html
- Yahoo! News Network. “Alertan sobre aparición de nuevo malware”, [Web en línea]. (23 de Octubre de 2011), [24 de Octubre de 2011]. Disponible en la Web: http://mx.noticias.yahoo.com/alertan-aparici%C3%B3n-malware-143000425.html

Referencia (Tabla 5.1)

- Softonic International S.L. “Antivirus”, [Web en línea]. (1997-2011), [25 de Noviembre de 2011]. Disponible en la Web: http://www.softonic.com/s/antivirus?ab=1