UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Facultad de Estudios Superiores Aragón

“Seguridad Informática:

Código Malicioso y Virus Informáticos”

Trabajo Escrito Bajo la Modalidad de
Seminarios y Cursos de Actualización y
Capacitación Profesional

Que para obtener el Título de

Ingeniero en Computación

Presenta:

GUILLERMO TERCERO ARMENDÁRIZ

Director de Tesis:
M. en C. Leobardo Hernández Audelo

San Juan de Aragón, Estado de México, Enero de 2008.

DEDICATORIAS

A mis padres:

Luis Tercero y Estela Armendáriz por la vida, por su ejemplo, por su cariño, por el esfuerzo en formarme y educarme, y por todo lo que significan para mí; viviré siempre agradecido. ¡Los quiero mucho!

A mis abuelos:

Jesús (†) y María de Jesús Tercero; Natalia (†) y Jesús Armendáriz, quienes supieron darme su cariño y su ejemplo. Los llevaré siempre conmigo.

A mis hermanos:

María Dolores y Marcos, por todos los momentos que hemos pasado, por su cariño, su apoyo en los momentos difíciles, las diversiones y las tristezas que tuvimos, y por estar siempre conmigo. ¡Gracias!

A mis sobrinos:

Yunuen Ailyn, Luis Enrique y Ari Gael para que llegado el momento, este trabajo les sirva como motivación para lograr sus metas. Supérense día a día.

A la familia Armendáriz:

Por la unión que siempre han mostrado.

A la familia Tercero:

Por su ejemplo de trabajo y dedicación.

A Fabiola:

Por todos los momentos que hemos compartido, por tu amor y tu confianza. TQM. Así como a la familia Olalde por haberme apoyado en los momentos difíciles y brindarme su amistad y confianza.

A Todos los que de alguna manera contribuyeron a este trabajo, y a quienes creyeron y confiaron en mí.

---

†

†

AGRADECIMIENTOS

Agradezco a la **Universidad Nacional Autónoma de México** por la formación que me brindó desde el bachillerato en la *Escuela Nacional Preparatoria Nº 9*, por la preparación que me dio durante mis estudios superiores en la *Facultad de Estudios Superiores Aragón* y por brindarme la oportunidad de cursar el Diplomado de Seguridad Informática en el CEM Polanco. Con esfuerzo y dedicación trataré de devolverle a la UNAM algo de lo mucho que me ha dado, así como mantener y enaltecer el prestigio que ostenta como la mejor Universidad de Ibero América.

Le doy las gracias también a los **Profesores** que se esforzaron por brindarme una formación de excelencia, característica de la Universidad Nacional y de la FES Aragón, especialmente a los profesores que amablemente dedicaron su tiempo y su esfuerzo en revisar este trabajo y en aportar su experiencia y conocimientos: *Mat. Luis Ramírez Flores, Ing. José Manuel Quintero Cervantes, M. en C. Jesús Hernández Cabrera y M. en C. Marcelo Pérez Medel.*

Hago también un reconocimiento muy especial a los **Instructores** que me impartieron cursos durante el Diplomado de Seguridad Informática, todos ellos de reconocido prestigio profesional y excelente calidad humana, quienes me han servido de ejemplo profesional y personal:

Dr. Enrique Daltabuit Godas
Investigador DGSCA UNAM y Coordinador Académico del Diplomado de Seguridad Informática

Dr. José de Jesús Vázquez Gómez
Jefe de la Oficina de Seguridad Informática del Banco de México, Académico e Investigador

M. en C. Guillermo Mallén Fullerton
Académico y Autor de Libros sobre Virus y Seguridad Informática

M. en C. José María Campaña
Consultor Independiente en Data Warehousing

Así mismo, a mis **Compañeros de Generación** con quien conviví durante mi estancia en la FES Aragón (y fuera de ella), principalmente a quienes me brindaron su apoyo incondicional y su amistad: Miguel Ángel Rafael Arellano, José Juan Pérez Rosas y Pedro Posada Almazán.

A mis **Compañeros del Laboratorio de Seguridad Informática**: M. en C. Leobardo Hernández Audelo, quien además de asesor, ha sido jefe, ejemplo, amigo y pilar importante para que este trabajo llegara a buen término. A quienes aportaron su paciencia, conocimientos y amistad dentro y fuera del laboratorio: Farah Berdeja, Eduardo Vega, Roberto Hernández, Omar y Marco León, Alberto Arce, Daniel Gachuz, Alejandro Arteaga, David Campos, Bruno Bedolla, Iván López, Rocío Núñez y a todos los que no menciono por nombre pero que han sido igualmente importantes.

A todos los que de alguna manera aportaron algo a este proyecto, creyeron y confiaron en mí.

¡Gracias¡

“La única computadora realmente segura es aquella que se encuentra apagada, guardada dentro de un bloque de concreto, en un cuarto sellado y custodiado por guardias armados, y aun así tendría mis dudas”.

Eugene H. Spafford
Dept.of Computer Sciences
Purdue University

ÍNDICE GENERAL

RESÚMEN.

Desde tiempos antiguos, la información ha sido un bien muy apreciado por el ser humano, ya que al adquirirla se tienen ciertas ventajas sobre los demás seres y se puede generar conocimiento nuevo. El proceso de manipular y transmitir información era, hasta hace algunos años, realizado en su totalidad de manera manual. Con el surgimiento de nuevas tecnologías, principalmente el cómputo, los procesos manuales se fueron automatizando de manera paulatina.

En la actualidad, el cómputo se ha extendido prácticamente a todas actividades cotidianas: operaciones financieras, comercio electrónico, transacciones bancarias, almacenamiento de expedientes clínicos, pago de impuestos, control de tráfico aéreo, actividades escolares o simple pasatiempo, como juegos en línea o foros de discusión.

La infraestructura para realizar todas estas operaciones son las computadoras y las redes, éstas últimas formadas por equipos de cómputo interconectado entre sí, lo que permite intercambiar información; dicho intercambio se realiza por canales públicos, por lo que se considera que la información viaja de manera insegura, ya que el canal es susceptible a ser intervenido por algún atacante que tiene la posibilidad de husmear, modificar o interceptar la información que pasa a través del canal.

Además, existen otros problemas de seguridad: el cómputo desde sus orígenes no contemplaba seguridad; existen usuarios (autorizados y no autorizados, internos y externos) que utilizando una computadora y la red, realizan fraudes financieros, roban información confidencial, acceden a computadoras gubernamentales y modifican la información en ellas contenida, realizan sabotaje; se debe mencionar también la existencia de código malicioso: virus, gusanos, spam (por mencionar solo algunos) que se difunde a través de la red a miles (quizá millones) de computadoras en el mundo y es uno de los problemas de seguridad más frecuentes y costosos.

La necesidad de proteger los recursos de cómputo (hardware, software e información) ha retomado importancia debido al incremento de incidentes de seguridad; pero, lo que agrava un poco el problema, es que en nuestro país no existe una cultura de la seguridad informática por parte de usuarios y administradores, la mayoría de las universidades no contemplan en sus planes de estudio alguna materia relacionada con seguridad en cómputo, y peor aún, no existen recursos humanos suficientes en cantidad ni en calidad como para hacer frente a la demanda creciente de personal preparado en el área.

Este trabajo representa un esfuerzo, no sólo de adquirir los conocimientos teóricos y prácticos que un diplomado universitario ofrece, sino también aplicarlos en la vida profesional. Se abordan, de manera general, los temas estudiados durante los módulos que comprende el *Diplomado de Seguridad Informática de la UNAM*, complementados con notas tomadas de libros especializados, apuntes, reportajes, comentarios y notas publicadas en periódicos, revistas y páginas de Internet de instituciones nacionales y extranjeras dedicadas a la seguridad.

Se busca en este trabajo dar un panorama general de la seguridad informática, desde sus inicios, evolución, fundamentos, problemática y alcances que tiene actualmente en diversas ramas del cómputo: Bases de Datos, Sistemas Operativos, Redes, así como técnicas de implementación y herramientas de seguridad.

Este trabajo hace especial énfasis en el tema que no ha dejado de evolucionar y que cada vez es más frecuente, dañino y costoso: El Código Malicioso. Se aborda el tema desde sus inicios y orígenes, así como sus principales componentes; se estudian los métodos utilizados para diseminar código malicioso, así como las Buenas Prácticas para erradicarlos. Se hace también una reseña de las tendencias futuras de los virus y código malicioso, tales como virus en teléfonos celulares y en sistemas de navegación en aviones, los mensajes spam, o los ataques phising.

Se espera, además, que este trabajo pueda servir como referencia para futuras investigaciones sobre seguridad, así como para los estudiantes y personas interesadas legítimamente en ampliar sus conocimientos sobre seguridad informática.

Este trabajo está integrado por 7 capítulos, cuyo contenido se describe a continuación. El Capítulo 1 "Antecedentes de la Información y la Seguridad" trata la historia de la información y la comunicación, proporciona un amplio panorama general de la evolución de la seguridad y sirve como introducción a los conceptos básicos manejados en esta disciplina; el capítulo 2 "Síntesis de la Seguridad Informática" resume los temas principales que esta disciplina contempla; se abordan temas como criptografía y sus aplicaciones, políticas de seguridad y control de acceso, seguridad en redes y en Internet, Seguridad en Bases de Datos y Sistemas Operativos, Protocolos y Herramientas de Seguridad, Sistemas de Monitoreo y Tendencias Futuras. El capitulo 3 "Código Malicioso y Virus Informáticos" aborda el tema de código malicioso en general, comenzando con los virus informáticos para luego abordar tópicos más recientes como spam o phising, ataques que prolifera en las redes de computadoras, y sobre todo, en Internet. El capítulo 4 “Programas Antivirus” hace un desglose de las utilidades y técnicas que utiliza un software antivirus para buscar y eliminar código malicioso, así como los métodos de actualización de las versiones antivirus. El capitulo 5 “Buenas Prácticas” menciona los métodos y procedimientos que pueden auxiliar a detener y erradicar un ataque de código malicioso. El capítulo 6 “Tendencias Futuras” aborda el tema de los futuros virus, las nuevas tecnologías y métodos de infección. En la parte de “Conclusiones” se describe el panorama actual tanto de la seguridad como del código malicioso. Así mismo, se incluyen un apéndice con un índice de figuras por cada capítulo y una breve descripción de las mismas.

1

ANTECEDENTES DE LA INFORMACIÓN Y LA SEGURIDAD

En este primer capítulo se describen los orígenes de la información, así como la historia y evolución de la comunicación. Se definen también los elementos que conforman a la seguridad informática y se revisa su evolución histórica hasta nuestros días; por último, se describe el entorno actual de la seguridad y sus conceptos básicos.

1.1 El Origen de la Información.

La *Información* es un conjunto de datos que le dan significado a algún fenómeno. Puede considerarse como un proceso en el que se adquiere y transmite conocimiento, y permite al individuo ampliar su visión del entorno. Dicho proceso se remonta a la época prehistórica, donde la adquisición de información se realizaba todos los días al apreciar los fenómenos naturales, y sólo podía efectuarse por medio de los 5 sentidos (gusto, olfato, oído, vista y tacto). Desde entonces, la información se convirtió en el bien más valioso, ya que de ella dependía, en gran parte, la sobrevivencia en el entorno.

Considerando a la información como un proceso, éste se compone de fases bien definidas, es decir, la primera de ellas es la *adquisición*, y se presenta cuando el individuo obtiene información sobre el entorno; posteriormente, vienen las fases de almacenamiento y organización, que derivan en *creación* de conocimiento nuevo conocido como *tecnología*, la cual es transmitida a otros individuos. La siguiente fase es el *almacenamiento*, que consiste en guardar y organizar información para recuperarla en cualquier otro momento a través de una *tecnología inversa*. Estas fases derivan en la generación de conocimiento nuevo, también llamado *tecnología*[1] (fig 1.1).

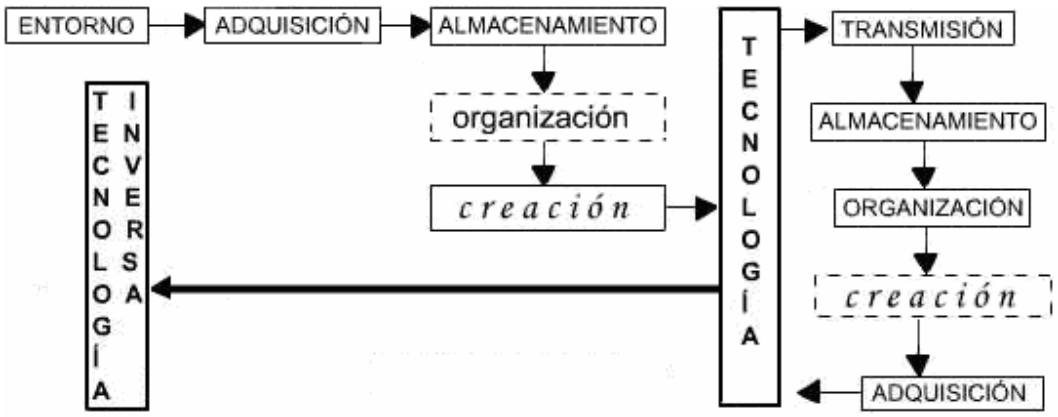


Fig 1.1. Fases de la Información.

La adquisición de información es posible a partir del desarrollo del cerebro humano, formado por células nerviosas llamadas “neuronas”, que han perdido la capacidad de reproducirse para dedicarse exclusivamente a comunicarse entre sí y con otras células. Durante la evolución, el sistema nervioso central se fue concentrando y compactando en la región cefálica, lo que permitió que la capacidad de almacenar información se incrementara notablemente.

[1] Tecnología. Del griego *tecno* y *logos*. Conjunto de conocimientos propios de una técnica; terminología exclusiva de una ciencia o arte. Fuente: Diccionario de la Lengua Española. www.rae.es

1.2 La Comunicación.

A medida que el individuo adquiere experiencias, las neuronas van estableciendo conexiones entre ellas; a mayor número de conexiones, es mayor la capacidad del cerebro, lo que permite el surgimiento del lenguaje. Los humanos establecen durante su primer año de vida, las conexiones neuronales que permiten adquirir, procesar, almacenar y transmitir información; el antecedente para el desarrollo del lenguaje en un niño, es la lengua que hablan los adultos que lo rodean; así, los bebés pueden discriminar contrastes vocales extranjeros, es decir, contrastes que no ocurren en su lengua materna y que no habían oído antes.

El lenguaje es un sistema convencional de hablar o escribir mediante símbolos, a través de los cuales, los seres humanos se comunican; es el primer medio eficiente de transmitir la información que se ha adquirido mediante los sentidos, y que se ha sistematizado y generado en el cerebro. Los lenguajes hablados fueron desarrollados por pequeños grupos de personas dentro de una comunidad para propósitos específicos (cazadores, médicos, astrónomos y demás), de ahí que unos cuantos podían experimentar y desarrollar vocabulario para su uso privado.

Con estos antecedentes se inicia, hace 100,000 años, la transmisión del conocimiento; hecho que transforma la capacidad de nuestra especie: ya no es necesario que cada individuo descubra una y otra vez lo mismo, porque la información se almacena y transmite por medio de canciones, poemas o discursos de generación en generación.

Por su parte, la escritura, es el medio que permite entender las expresiones de las civilizaciones antiguas, como por ejemplo, los colmillos de mamut labrados por el hombre de Neandertal hace 45,000 años, o el arte rupestre de hace 31,000 años. A través de estos y otros vestigios, se sabe que los sistemas notacionales de escritura datan de hace unos 18,000 años. El primer escrito conocido se atribuye a los sumerios de Mesopotamia, está escrito con caracteres ideográficos (caracteres que expresaban ideas y no palabras), y data del año 3000 a.C.

Poco a poco, la escritura fue evolucionando. Por ejemplo, los egipcios escribían con jeroglíficos, signos que representaban sonidos o palabras, pero no letras. Luego, los pueblos semíticos de Siria y Palestina tomaron el silabario egipcio bajo una forma más sencilla y reducida. Más tarde, los griegos tomaron la escritura de los fenicios, separaron vocales de consonantes y las escribieron por separado, llegando a la escritura alfabética hacia el 800 a.C.; ahora se necesitan sólo unas decenas de símbolos para leer y escribir.

Cuando el hombre tuvo la capacidad de comunicarse de manera escrita, surgió la necesidad de proteger, almacenar y transmitir información de manera confidencial, lo cual dió origen a la *criptología* (ciencia para ocultar información), que se estudiará en el capítulo 2 de este trabajo.

1.3 Almacenamiento de Información.

El hombre de la antigüedad no tenía forma de almacenar el conocimiento, porque no contaba con los medios adecuados; con la invención de la escritura, junto con la tela y el papel, se dio el gran salto hacia los primeros métodos de almacenamiento: rollos y libros.

Ya con los medios adecuados y a partir de la necesidad de almacenar información, se funda hace 2300 años la biblioteca de Alejandría; en ella se reunieron 700,000 títulos en alrededor de 200 años, dando paso a la primera gran biblioteca del mundo. Gracias a esta concentración de conocimiento, se formaron entorno a la biblioteca, grupos científicos, literarios y filosóficos, antecedentes de las universidades actuales.

En el año 40 a.C. se quema la biblioteca principal y más tarde es destruido el edificio colindante, los pocos libros que sobrevivieron pasaron a las colecciones de los conventos y los palacios, donde el acceso era difícil; los estudiosos tenían que viajar de una colección a otra para obtener conocimientos; obtener copias era caro, y la integridad de los textos era mínima por tratarse de traducciones de otros idiomas.

Sin embargo, los árabes en Alejandría habían acumulado una amplia colección de traducciones que llevaron a sus ciudades de origen, lo que preservó gran parte del conocimiento, que luego regresó a Europa aumentado y refinado. Con ello, se originó en los siglos XV y XVI la Época del Renacimiento, en la que se tuvo acceso más fácil a la información, motivando que se fundaran las primeras universidades y bibliotecas.

El conocimiento generó nuevas tecnologías, reflejadas a través de nuevos inventos, como la imprenta de tipografía móvil, dispositivo mecánico que permite realizar copias de textos impresos en tela o papel en cantidades nunca antes logradas. Con ello, el conocimiento deja de ser elitista, ya que se hace llegar a todo el mundo.

Después de varias épocas caracterizadas por avances tecnológicos y métodos de producción cada vez más eficientes, en el siglo XX, dichos avances se presentan en todas las ramas del conocimiento, con lo que surgen nuevos inventos; de ellos, el más relevante es el cómputo, lo que provoca que la información deba ser codificada cuando se almacena, procesa o transmite usando computadoras.

El código que se utiliza en cómputo emplea dos elementos: el 0 (estado apagado) y el 1 (estado encendido) para expresar cualquier texto, imagen, sonido o entidad aritmética. Una sucesión de 1’s y 0’s recibe el nombre de "*archivo";* cada símbolo (*cero* o *uno*) es un bit, y una secuencia de 8 bits se llama *byte* (*octeto*). Así, es posible codificar 256 (igual a 2x2x2x2x2x2x2x2) caracteres distintos (mayúsculas, minúsculas, números y caracteres especiales) empleando todos los posibles octetos. Las computadoras permiten olvidar el alfabeto (26 signos) y utilizar solo 2 (0, 1) para el procesamiento de datos.

Por su parte, gracias al *electromagnetismo* se realizan las operaciones de manejo de información digital: almacenar, transmitir o manipular. Se obtiene una cadena de bits formada por ceros y unos, y esta cadena es la información que se respalda, se cifra a binario, se transmite, manipula y almacena.

Actualmente ya no se requiere almacenar información impresa a través de material bibliográfico en estantes dentro de bibliotecas o hemerotecas; ahora solo se requiere "digitalizar" la información, es decir, convertirla en una serie de 1's y 0's para que pueda ser legible en formato digital y almacenarla en algún medio magnético.

1.4 Antecedentes de la Seguridad.

Desde los inicios de la humanidad, la seguridad ha jugado un papel fundamental, tanto en la vida diaria como en los conflictos bélicos; con la invención de la escritura, la seguridad fue utilizada en mayor medida, lo que produjo su desarrollo de manera notable.

1.4.1 Inicios de la Seguridad.

La primera aplicación criptográfica conocida son los jeroglíficos egipcios, que se remontan a 4000 años atrás y se utilizaban para narrar la vida de sus faraones. Más tarde, en Mesopotamia, cerca del año 1500 a.C. se elaboró en una tableta que contiene una fórmula cifrada para producir vidriado para cerámica. Varios pueblos de la antigüedad emplearon diversos métodos de cifrado, como los griegos, espartanos y hebreos.

Entre los años 500-600 a.C., un escribano hebreo que trabajaba en el libro de Jeremías, usó un cifrado sencillo invirtiendo el alfabeto (cifrado de substitución). En el año 487 a.C., los griegos inventan un dispositivo llamado skytale, un bastón al que se enrollaba un cinturón de cuero sobre el cual se escribía el mensaje, sólo alguien con un bastón del mismo diámetro podía leer lo escrito (fig. 1.2).

Fig 1.2. Skytale.

Entre los años 50-60 a. C., el emperador romano Julio César utilizó un sistema de cifrado basado en sustitución simple, es decir, desplazando el alfabeto unos cuantos caracteres en el alfabeto[2]. Desde entonces, este método es conocido como "Cifrado César" en honor a su inventor.

Por otro lado, el libro indú *"Kamasutra de Vatsayana"*, escrito entre el año 0 y el 400 d.C. (¿?), menciona a la criptografía como los yogas 44 y 45 de los 64 que deben conocerse y practicarse. En esta lista se lee que la criptografía es *"el arte de entender la escritura cifrada, de escribir palabras en forma peculiar y pronunciarlas en forma peculiar"*.

Más tarde, la criptografía se tornó importante durante la Edad Media, cuando los gobiernos se comunicaban con sus embajadores por medio de mensajes cifrados; por ejemplo, en 1453, el gobierno Italiano establece un grupo dedicado exclusivamente al estudio de la criptografía. Más tarde, la llegada del telégrafo significó un importante avance, que derivó en la creación de máquinas electromecánicas para cifrar mensajes.

Después de la Primera Guerra Mundial, las técnicas de ocultamiento de información se usaron ampliamente, lográndose avances como el descubrimiento hecho por Gilbert S. Vernam del algoritmo de cifrado *OTP*[3] que genera una llave que se utiliza sólo una vez.

[2] Este procedimiento será descrito más adelante en este trabajo.
[3] OTP: siglas en inglés de "One Time Pad"

El 1 de septiembre de 1939, con la invasión nazi a Polonia se inicia la Segunda Guerra Mundial, época en la que la seguridad y la criptografía toman un auge espectacular, y en la que alcanzan su clímax los cifrados por sustitución y las máquinas cifradoras. Las técnicas de ocultamiento de información también se aplicaron en las relaciones diplomáticas, en secretos comerciales e industriales, e información científica.

1.4.2 El Cómputo y sus Problemas de Seguridad.

La historia del cómputo se divide en periodos definidos por los avances tecnológicos que presentaban las computadoras, sus diversos componentes o sus usos.

La *Primera Generación* de las computadoras inicia en la década de los 50's, donde se utilizaba tecnología a base de tubos de vacío (bulbos). El manejo de los equipos era a través de instrucciones en lenguaje ensamblador y los equipos eran tan grandes como un edificio; el equipo periférico se limitaba a lectoras, perforadoras de tarjetas y cinta de papel, los sistemas eran centralizados y de propósito específico. El precio del equipo era de un millón de dólares, por ello sólo el gobierno o compañías grandes podían tenerlo.

En este periodo surge la computadora ENIAC[4], que ejecuta un programa a la vez, es decir, si varios usuarios requieren el uso de los recursos, se inicia y termina con el primer trabajo presentado, luego se procesa el siguiente y así sucesivamente. La entrada de programas y datos se realiza mediante tarjetas perforadas, y la salida mediante listados impresos; es decir, mientras se leen las tarjetas y se imprimen los listados, el procesador está ocioso. La protección que requería la información pudiera parecer sencilla en la actualidad, ya que sólo existía seguridad física hacia el equipo, sin embargo, en este periodo se establece la oficina COMSEC (Communications Security), encargada de investigar el espionaje eléctrico-electrónico a través de intercepción de radiaciones.

La *Segunda Generación* inicia a finales de los 50's, caracterizada por el uso de tubos de vacío miniaturizados, transistores y el surgimiento de los lenguajes de programación. Al observar los problemas provocados por procesar un programa a la vez, se usan computadoras pequeñas para realizar las operaciones de entrada y salida, es decir, se colocaban varios programas y datos en dispositivos de almacenamiento más rápidos (cintas), pero como los programas no se escribían con eficiencia óptima, en la ejecución de los mismos, el procesador (y otros recursos) seguían ociosos.

Durante la *Tercera Generación*, las computadoras utilizaban circuitos integrados y tecnología semiconductor; además, se diversifican los lenguajes de programación numéricos y no numéricos, y surgen los sistemas operativos (S.O.). En 1964 se lanza el *Sistema/360* de *IBM* y se implementa la primera red local (LAN), en 1968 se implementa la primera red amplia (WAN) conocida como ARPAnet. En 1967 el DoD [5] lanza el primer estudio de amenazas para sus computadoras, aparecen las minicomputadoras y se inicia el uso de las telecomunicaciones.

[4] Electronic Numerical Integrator and Computer
[5] DoD: Department of Defense, Departamento de Defensa de los Estados Unidos de América.

En la *Cuarta Generación,* iniciada en 1970, los equipos emplean Circuitos Integrados de Gran Escala[6] y surgen las bases de datos y los procesadores.

Con el proyecto *"Multics"* surgen los conceptos de "tiempo compartido" y "multitareas", que asigna recursos en forma alternada a varios programas para evitar el ocio de los dispositivos; con el uso de estos nuevos esquemas inicia la "Era de la Seguridad en Cómputo", ya que si se comparten recursos (procesador, memoria, impresora) un programa malicioso puede enterarse de los datos y operaciones que está realizando un programa que se esté ejecutando "simultáneamente".

A mediados de los años 70's, se lanza al mercado la *Altair 8800*, considerada como la primera computadora personal, la cual cuenta con microprocesador Intel 8080 y 256 bytes de memoria. En 1977 se realiza la primera implementación de *TCP*[7], protocolo que dio origen a *Internet Protocol (IP)*. En 1979, *Xerox, DEC* e *Intel* anuncian "*Ethernet*[8]*"*, diseño de red que permite a computadoras heterogéneas comunicarse en una red local. Más tarde, se lanzan la *Personal Computer (PC)* y los sistemas *Apple*, las dos grandes tendencias comerciales de la época, con lo que se inicia la *"Época Dorada de la Computación"*, ya que el cómputo llegaría a estar al alcance de toda la gente.

Con el auge de la seguridad en cómputo, surge también el primer modelo matemático para políticas de seguridad multinivel, desarrollado por Bell y LaPadula (descrito más adelante). Además, inicia sus labores la ARPA[9]; y se comienzan a utilizar *Team Triggers*, equipos de trabajo encargados en verificar la seguridad de los sistemas y hacer pruebas de penetración; también se utilizan las técnicas de "parches" para acotar debilidades, pero como los sistemas seguían siendo penetrables, surge el "Monitor de Referencia"[10].

El uso cada vez mayor de las computadoras, aunado al cableado directo o por línea telefónica, derivó en el crecimiento de las redes, provocando mayores y más graves problemas de seguridad: ahora la información se encuentra alojada en cientos de equipos dispersos, se puede compartir y transmitir por canales públicos e inseguros; es decir, existen más recursos de cómputo y más formas de perderlos.

En los 90's, las organizaciones usaban servidores *"mainframe"*, donde alojaban todas las aplicaciones e información de la compañía, porque era mas fácil administrar un solo equipo; pero la carga de trabajo del servidor se distribuyó en varias máquinas, provocando que el control sobre programas, la seguridad de datos, documentación del sistema, respaldos y planes de recuperación tuvieran que ser aplicados ahora en varios equipos.

[6] Conocidos en inglés como "LSI" ó Large Scale Integration
[7] *Transport Control Protocol* ó Protocolo de Transporte y Control, base para la comunicación en cómputo.
[8] Nombre formado por las palabras *"eter"*, que en la química clásica hace referencia a la "sustancia que ocupa todos los espacios vacíos" y "net", que en inglés significa red.
[9] Advanced Research Project Agency que desarrolla ARPANet, red de computadoras precursora de Internet.
[10] Conocido también como Security Kernel, abstracción que permite a "sujetos" acceder a "objetos", y se interpone entre ellos por seguridad.

Por su parte, los problemas en las computadoras personales también aumentaron, debido a que no cuentan con protecciones mínimas, provocando el robo de partes físicas, infecciones por virus, dispersión de la información en cientos de equipos, pérdida de información por falta de respaldos oportunos, entre muchos otros.

El crecimiento de las redes produjo inquietud en el gobierno de Estados Unidos, quien comenzó a desarrollar investigaciones que buscaban comunicar los centros militares con las universidades; la red debía seguir funcionando a pesar de que uno (o varios) de sus elementos fueran destruidos. El proyecto (ARPA) se llevó a cabo con éxito y debido a su crecimiento insospechado, llegó a crecer a ritmo mayor que la red telefónica en los años 90's, lo que derivó en el surgimiento de Internet, que por su forma de trabajo dificulta el mantener la confidencialidad y aumenta el riesgo de ataques.

Por otro lado, las organizaciones, al no contar con un área de seguridad en cómputo, provocan que el administrador de la red, además de sus tareas diarias, deba verificar los problemas de seguridad, y al ocupar demasiado tiempo resolviendo problemas y los pobres conocimientos de seguridad, facilita los ataques a la red. Además, a los proyectos de sistemas se les asignan recursos (tiempo y dinero) limitados, aunque la seguridad casi nunca es considerada.

1.5. Concepto de Seguridad Informática.

Hoy en día, los sistemas de cómputo son fundamentales para la seguridad de una organización, e incluso de un país; por ello es que algunos consideran a la seguridad informática como un *arma de guerra,* de ahí la importancia de analizar sus elementos y alcances, para definir las soluciones más adecuadas.

La *seguridad* en general se puede entender como una cualidad que implica "libre de riesgo", "certeza", "confianza". Por *Seguridad Informática* se entiende a la forma de adquirir, almacenar, procesar y transmitir información en un entorno de red, y asignarle, lo más posible, las cualidades de integridad, confidencialidad, autenticidad y disponibilidad. Se considera entonces, que la información es segura cuando el costo de romper la seguridad excede el valor de la información asegurada, o que el tiempo requerido para romper la seguridad excede el tiempo de vida útil de la información.

Así, un *Sistema de Cómputo* es un conjunto formado por hardware, software, medios de almacenamiento, información y personas involucradas en el manejo y administración del mismo; en el ámbito de seguridad, los principales recursos que hay que proteger son hardware[11], software[12] y datos[13].

En este contexto, se entiende por *Compromiso de Seguridad* a cualquier forma posible de pérdida o daño en un sistema de cómputo; por lo tanto, *comprometer la seguridad* equivale a la posibilidad de provocar pérdida o daño.

[11] Conjunto de componentes que integran la parte material de una computadora. Fuente: Diccionario de la Lengua Española. www.rae.es

[12] Conjunto de programas e instrucciones para ejecutar ciertas tareas en una computadora. Fuente: IDEM.

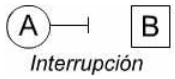
[13] Dato: Información dispuesta de manera adecuada para su tratamiento por ordenador. Fuente: IDEM

Por su parte, una *Vulnerabilidad* es cualquier debilidad que puede explotarse para causar pérdida o daño al sistema.

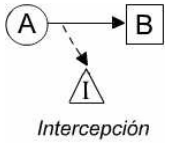
A su vez, una *Amenaza* es cualquier circunstancia capaz de provocar pérdida o daño en el sistema, y puede ser de 4 tipos, representados gráficamente en las figuras siguientes, donde:

A = Fuente u origen de los datos, remitente
B = Destino de los datos, receptor
= Intruso, atacante.

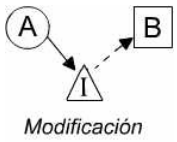
El *Flujo Normal* de datos considera que A origina un mensaje, se envía por el canal público y llega a B sin alteraciones, sin pérdida, y sin que el atacante pudiera tener acceso a los datos. A pesar de que existen diversas amenazas y vulnerabilidades, no se consuma ataque alguno.



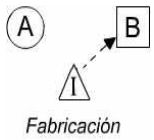
La *Interrupción* ocurre cuando el sistema o sus activos se pierden o quedan no disponibles. El borrado (accidental o intencional) de datos, la destrucción o daño de un dispositivo de hardware, o la falla (provocada) en la comunicación en la red, son ejemplos de ello.



La *Intercepción* de datos se presenta cuando una parte no autorizada (persona, proceso o sistema de cómputo) logra tener acceso a un activo del sistema. Ejemplo de ello es el copiado (ilícito) de programas o archivos, o la intervención del canal para obtener datos sobre la red.



La *Modificación* ocurre cuando una parte no autorizada accede y manipula a voluntad un activo del sistema. Si un intruso modifica una base de datos, altera un programa para que realice una operación distinta a la normal, o modifica datos en una comunicación, se trata de algún tipo de modificación.



La *Fabricación* de datos existe cuando una parte no autorizada puede producir objetos falsos en un sistema de cómputo. La inserción de transacciones falsas en una red o agregar registros adicionales a una base de datos, son considerados como fabricación.

Por lo tanto, un Ataque a un sistema de cómputo es la acción de explotar una vulnerabilidad; generalmente se realiza en dos etapas, la primera se llama *Ataque Pasivo*, y consiste en sólo observar comportamientos o leer información sin alterar el estado del sistema ni de la información, afectando sólo la confidencialidad. El fisgoneo de mensajes o el análisis de tráfico sobre una red, se consideran ataques pasivos.

La segunda etapa es el *Ataque Activo*, donde el atacante cuenta con la capacidad de modificar o alterar información, el estado de sistema, o ambos; con ello se afecta tanto la confidencialidad, integridad y autenticidad de la información, como por ejemplo: el engaño, la suplantación, réplica y modificación de mensajes o la negación de servicio.

Cuando se habla de comunicaciones abiertas (como Internet), se asume que siempre está presente un atacante con la capacidad para realizar cualquier acción sobre la información: interceptar, leer, alterar, modificar, cambiar, fabricar, retener o reenviar; se asume también que el atacante conoce los algoritmos[14] de seguridad y su implementación; en ambos casos, su objetivo es aprovechar en su favor la información, el medio o los recursos de cómputo.

Por lo anterior, la seguridad de la información no debe basarse en el ocultamiento del algoritmo de seguridad que se utiliza, es decir, no debe existir "*security by obscurity*" como premisa. En cambio, las herramientas utilizadas en seguridad deben ser públicas, tanto en su algoritmo como en su implementación, ya que la seguridad siempre debe residir en la fortaleza del algoritmo y no en el hecho de mantenerlo oculto.

1.5.1 El Modelo OSI y su Arquitectura de Seguridad.

La OSI[15] se encarga de realizar las normas para ciertos procedimientos; en el caso de la seguridad informática, cuenta con la norma ISO 7498-2, que además de los conceptos básicos, da a conocer los *servicios de seguridad* que definen los objetivos específicos de la seguridad, así como los *mecanismos de seguridad,* que consisten en una funcionalidad específica para implementar servicios de seguridad.

Es decir, los *mecanismos de seguridad* son procedimientos que sirven para implementar un servicio de seguridad, o sea, especifican "cómo lograrlo"; mientras que, un *servicio de seguridad* es una característica que debe tener un sistema para satisfacer una política de seguridad, o sea, definen "lo que es requerido". De esta forma, la Arquitectura de Seguridad OSI identifica 5 servicios de seguridad:

La *Confidencialidad,* que busca garantizar que la información sólo sea accedida por las partes autorizadas; este servicio y su implementación constituyen uno de los objetivos de la seguridad informática, y para implementarlo, se usa principalmente a la criptografía.

La *Autenticación* tiene como objetivo garantizar que las entidades participantes en una comunicación sean las que dicen ser, es decir, identifica una parte ante las demás, de manera incontroversial y demostrable. La autenticación se clasifica en tres tipos de acuerdo a la naturaleza de los elementos que la implementan:

en *algo que se sabe* (como una contraseña)*,*
en algo que se tiene (como una llave)*,*
en algo que se es (alguna característica corporal o física)*.*

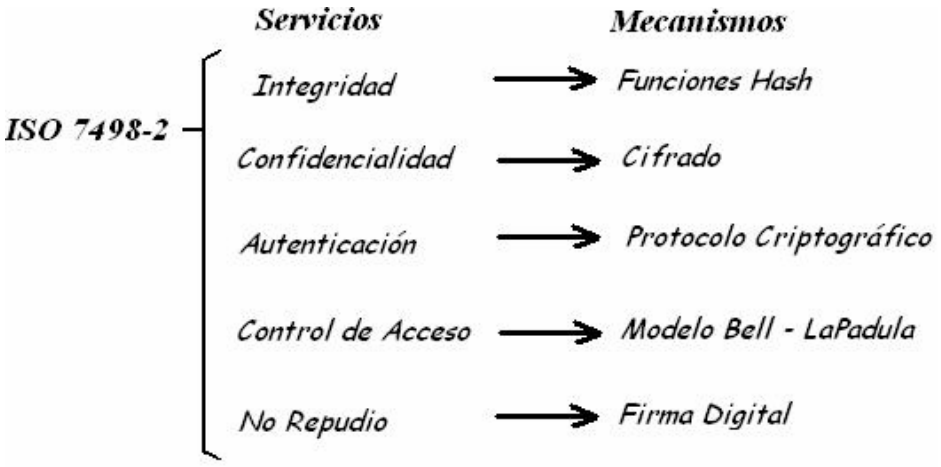
La *Integridad* es el servicio que protege a los activos del sistema contra modificaciones, alteraciones, borrado o inserción; se implementa principalmente a través de funciones *hash,* un tipo de criptografía que no utiliza llaves.

[14] Conjunto ordenado y sistematizado de operaciones que permite hallar la solución de un problema.
[15] OSI o ISO, International Standard Organization, es la organización que se encarga de implementar normas para procedimientos y dispositivos de comunicación.

El *Control de Acceso* es un servicio que protege los activos del sistema contra accesos y uso no autorizados; no se utilizan técnicas criptográficas para su implementación porque existen técnicas propias y modelos específicos para ello. Este servicio está cercanamente relacionado al de autenticación, ya que un usuario debe ser autenticado antes de tener acceso a los activos del sistema.

El servicio de *No Repudio*, se utiliza cuando se efectúa una comunicación entre dos entidades y busca garantizar que ninguna de las dos partes niegue haber tenido parte en esa comunicación. Para implementar este servicio se utilizan esquemas de llave pública, como las *firmas digitales, y cifrado de llave pública* y *de llave privada* (utilizando en esta última, una tercera parte confiable).

Así, la relación entre Servicios y Mecanismos se da de la siguiente forma:



1.5.2 El Triángulo de Seguridad.

Algunos especialistas consideran que los servicios de confidencialidad, integridad, y disponibilidad forman el "Triángulo de Oro de la Seguridad" (fig 1.3).

Para preservar la confidencialidad y la integridad, se utiliza el control de acceso, pero un punto de acceso único no puede garantizar completamente la disponibilidad. De hecho, los mayores éxitos en seguridad se han tenido en lo relativo a la confidencialidad e integridad; mientras que, la protección para la disponibilidad no ha sido posible lograrla hasta ahora.

Fig 1.3. El Triángulo de Seguridad

La seguridad informática distingue dos ámbitos bien definidos:

1. Los especialistas en seguridad, encargados del resguardo de material clasificado y material sensible pero no clasificado, así como de todos los elementos del sistema, como recursos, dispositivos, e incluso, los recursos humanos.

2. En contraparte se encuentra el usuario común, que se preocupa por cuestiones como: ¿quién tiene información acerca de mí?, ¿quién está usándola o puede usarla?. La información relacionada con este ámbito incluye datos personales (edad, teléfono y dirección), información crediticia o médica, historial comercial, entre otras más.

De esta manera, las violaciones a la confidencialidad se realizan a través del monitoreo e intervención de canales de comunicación y de la obtención de información clasificada y general, mientras que las violaciones a la Integridad se efectúan por medio de la alteración de registros de información. Las violaciones a la Disponibilidad consisten en robo de tiempo de procesador (ciclos de reloj), negación de servicio (impedimento de usar los recursos y la información), entre otros.

En este Capítulo I se ha presentado una introducción histórica, conceptos básicos entorno a la Seguridad Informática, así como un breve panorama actual. En el Próximo Capítulo se presenta una síntesis sobre los temas más importantes que estudia la Seguridad Informática.

2

SÍNTESIS DE LA SEGURIDAD INFORMÁTICA

En el capítulo anterior se revisaron los antecedentes históricos de la información y la comunicación, así como los principales conceptos empleados en seguridad. En el presente capítulo se revisan los temas estudiados por la seguridad informática, abordando principalmente los fundamentos de la criptografía y sus aplicaciones actuales.

2.1 Criptografía.

Cuando el hombre inventó la escritura, surgió la necesidad de mantener protegida la información; a partir de esa necesidad surge la *Criptografía*[16], ciencia que se encarga de mantener segura la información, transformando la información legible (texto claro) en información ilegible (texto cifrado), a través de un elemento único (llave), de tal forma que sólo el poseedor de la llave pueda entender el texto cifrado. En contraparte, el Criptoanálisis, busca recuperar el mensaje en claro sin poseer la llave; ambas ciencias, criptografía y criptoanálisis, forman parte de una ciencia genérica llamada Criptología[17].

La criptografía se basa en algoritmos de cifrado (funciones matemáticas) para cifrar y descifrar un mensaje. Así, el cifrado de datos es el proceso de transformar un mensaje (M) para ocultar su contenido, obteniendo el mensaje cifrado (C); mientras que el descifrado es el proceso de regresar un mensaje cifrado (C) a texto en claro (M).

La implementación de un algoritmo de cifrado incluye: el mensaje en claro (M), una llave de cifrado (Kc), el proceso de cifrado, texto cifrado (C), proceso de descifrado y la llave de descifrado (Kd) (Fig 2.1). De esta forma, para cualquier mensaje en claro (M), cifrado con la llave (K) que produce el texto cifrado (C), se denota como **Ek(M) = C**, mientras que el descifrado de (C) con llave (K), que recupera (M) es **Dk(C) = M.**

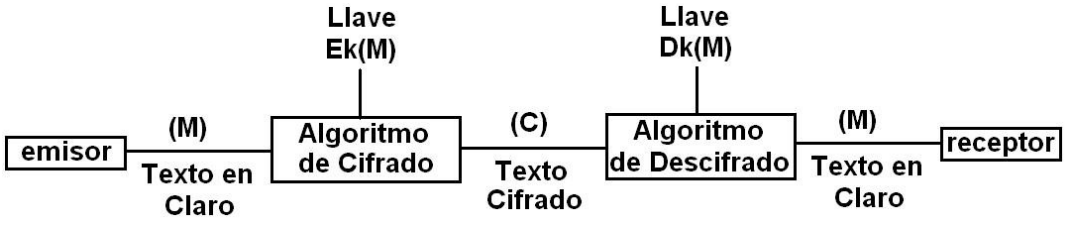


Fig 2.1. Proceso de Cifrado y Descifrado

Así, tanto el proceso de cifrado como de descifrado forman un Criptosistema (fig 2.2):

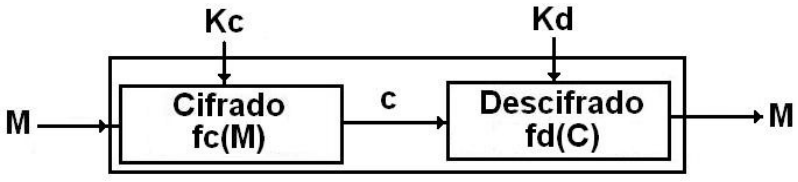


Fig 2.2. Criptosistema

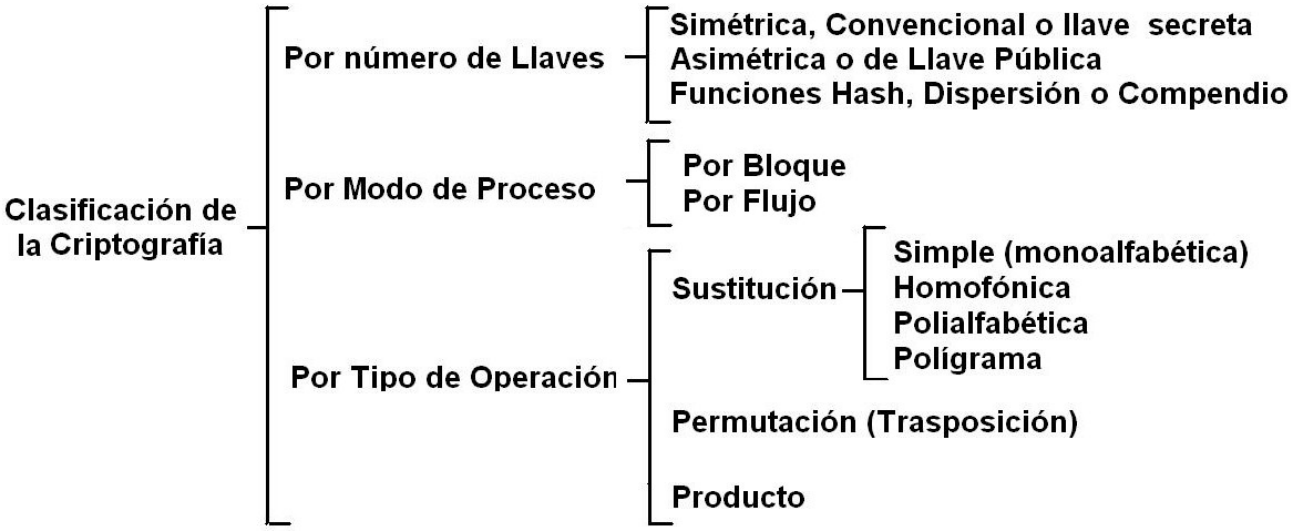
[16] Proviene de *kriptos:* esconder y *grafos:* estudio; "Estudio de la escritura escondida".
[17] Proviene de *kriptos:* esconder, *logos:* estudio; "Ciencia de ocultar la información".

La criptografía implementa cuatro servicios de seguridad: *integridad*, *confidencialidad*, *autenticación* y *no repudio* (descritos en el capítulo anterior) y se basa en el uso de llaves de un gran espacio; por ejemplo, una llave de 1024 bits, produce un espacio de 2^{1024} posibles llaves. Los algoritmos de cifrado basan su complejidad en la importancia de la información que protegen; así que, mientras más valiosa es la información, más complicado es el algoritmo de seguridad que se implementa. Para su estudio, la criptografía se clasifica de acuerdo a ciertos criterios:

Si se toma en cuenta el Número de Llaves, se trata de "Criptografía Simétrica" (usa una única llave secreta para cifrar y descifrar) o "Criptografía Asimétrica" (que utiliza dos llaves: una pública y una privada, de forma que lo que se cifra con una llave, se descifra con la otra y viceversa); también se encuentran las "Funciones Hash", que no utilizan ninguna llave, sino que son funciones matemáticas de entrada variable y salida fija.

Si se considera al Modo de Proceso, la criptografía se divide en "Cifrado por Bloque" (cuando la información se cifra en bloques de longitud fija, es decir, cada determinado numero de bytes de un mensaje) o "Cifrado por Flujo" (si se procesa la información como un flujo de bytes, independientemente del tamaño del mensaje).

Si se considera al Tipo de Operación, se habla entonces de Sustituciones (mapeo de caracteres), Permutaciones (arreglo de caracteres), u operaciones Producto (combinación de las dos anteriores). Así, la clasificación de la criptografía, de acuerdo a sus diferentes criterios, se muestra en el siguiente cuadro:



En este trabajo se utiliza la clasificación de acuerdo al número de llaves.

2.1.1 Criptografía Simétrica.

Se conoce también como *criptografía simétrica, convencional* o d*e llave secreta* debido a que entre el emisor y el receptor debe existir un acuerdo de llave previo (que se debe mantener secreta); dicha llave se utilizará para cifrar y descifrar, de modo que si se compromete, la seguridad se viene abajo.

Así, cada caracter de M se reemplaza por un caracter *k* posiciones a la derecha (corrimiento) en el alfabeto, aunque también se pueden emplear operaciones elementales, como permutaciones y combinaciones. La criptografía simétrica incluye a los algoritmos clásicos como César, Vigenere, Hill o Playfair; además de los algoritmos aceptados como estándar mundial como DES (Data Encryption Standard, 1977), 3DES, IDEA (International Data Encrption Algorithm, 1990) y AES (Advanced Encryption Standard, 2002).

Entonces, para que dos entidades (A y B) puedan intercambiar un mensaje cifrado, necesitan acordar previamente una llave; dicho acuerdo puede parecer sencillo, aunque en realidad acarrea algunos problemas graves, como el hecho de poder intercambiar la llave sin que pueda ser interceptada por un intruso, además de que se debe garantizar que la llave viene del emisor legítimo; por otro lado, si varias entidades están involucradas en el intercambio y alguna llave se compromete, se tendrían que volver a intercambiar todas las llaves previamente acordadas, sin considerar que si el número de entidades aumenta, deberán hacerse más intercambios, como se muestra (fig. 2.3):

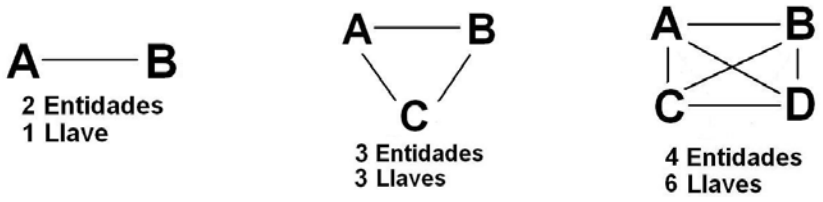


Fig 2.3. Relación entre Entidades con Respecto al Número de Llaves.

Por tanto, el intercambio crece a razón de $nk = ne(n-1) / 2$

donde: ***nk*** = número de llaves
ne = número de entidades.

Analizando este planteamiento, se comprueba que son graves los problemas que acarrea el uso de criptografía simétrica, principalmente en cuanto a administración de llaves (revocación, emisión, y almacenamiento); sin embargo, a partir de la búsqueda de la solución a estos problemas, surge un nuevo tipo de criptografía.

2.1.2 Criptografía Asimétrica.

En 1977, los investigadores de *Stanford University*, Witfield Diffie y Martin Hellman, publicaron el documento *"New Directions In Cryptography"* que buscaba dar solución a los problemas derivados del uso de Criptografía Simétrica y que introdujo por primera vez el concepto de "Criptografía de Llave Pública", un método matemático para intercambio de llave, que derivó en la implementación de la "Criptografía Asimétrica".

En este esquema, cada participante tiene dos llaves: una *Pública* (que todo el mundo conoce), y una *Privada* (que solo conoce él mismo). Para enviar información cifrada, el emisor usa la llave pública del receptor, quien es el único que puede descifrar el mensaje mediante su llave privada, ya que los mensajes cifrados con la llave pública no se pueden descifrar con la llave privada, ni viceversa. De esta forma, se implementa autenticación y confidencialidad, y sobre todo, no se requiere acuerdo previo de llave.

Por otro lado, se reduce el número de llaves a distribuir, ya que, una comunidad de *n* entidades que usa esquemas de llave pública sólo requiere *n* llaves privadas y *n* llaves públicas, es decir, un total de ***2n*** llaves, a diferencia de los esquemas de llave simétrica.

A pesar de sus ventajas, este esquema acarrea ciertos problemas, como los relacionados con la administración de llaves; además, es susceptible a ataque "por hombre en medio", donde un intruso se hace pasar por el emisor ante el receptor, y por el receptor ante el emisor, engañando a ambos; aunque, el problema principal, es que resultan computacionalmente muy costosos por la cantidad de cálculos que deben efectuarse.

En 1978, *Rivest, Shamir* y *Adleman,* usando matemáticas para resolver problemas criptográficos, diseñan el primer sistema práctico de cifrado de llave pública y firma, conocido como RSA (por las siglas de sus creadores); con ello, se revitalizaron los esfuerzos para encontrar métodos de cifrado más eficientes. Durante la década de los 80's se vislumbraron mayores avances en esta área, pero fue hasta 1985 cuando *ElGama*l encontró otro potente y práctico sistema de llave pública (que lleva su nombre), por lo que este método se convertiría en estándar mundial.

2.1.3 Funciones Hash.

Son funciones matemáticas unidireccionales (fáciles de calcular en una dirección, pero infactible en la otra), que aceptan entradas arbitrariamente grandes y entregan una salida de longitud fija y pequeña. Se usan para verificación de integridad, ya que si se cambia un bit de la entrada, cambia completamente la salida; por eso se considera que un valor hash es una "huella digital" de un mensaje. Además, se considera infactible que dos entradas lleven al mismo valor hash, y que dado un valor hash se pueda hallar más de una entrada.

Los algoritmos hash principales son MD5, SHA-1 (con dos variantes, conocidas como SHA-256 y SHA-512), RIPEMD, N-Hash, Snefru, Tiger, Panama y Haval.

2.1.4 Esteganografía

Es una disciplina que se encarga de esconder mensajes dentro del mismo texto en claro pero sin hacer transformación alguna; no forma parte de la criptología, pero es importante conocerla. En este caso, la seguridad se basa solo en ocultar el secreto ('seguridad por oscuridad'), como las marcas de agua en los billetes, la microfotografía o la tinta invisible.

2.2 Políticas de Seguridad

La seguridad informática se implementa a partir de ciertos criterios, que a veces no son claros o fáciles de medir. En la actualidad existen organismos públicos y privados cuya finalidad es dar a conocer estos criterios y difundirlos, uno de ellos es el SANS[18], que a partir de encuestas define los principales errores de los directivos de sistemas, conocidos como "Pecados Capitales", que quedaron listados como sigue:

1. Suponer que los problemas desaparecen si no se les hace caso.
2. Autorizar soluciones reactivas y parches de corto plazo, por lo que los problemas reaparecen rápidamente.
3. No saber cuánto dinero vale la información y qué tanto depende de ella la reputación corporativa.
4. Depender principalmente de un firewall[19].
5. No lidiar con los aspectos operacionales de la seguridad.
6. Aplicar sólo unos cuantos parches y no dar seguimiento para verificar de que los problemas en verdad estén resueltos.
7. No entender la relación entre seguridad y los problemas de funcionamiento.
8. Entender la seguridad física, pero no las consecuencias de una mala seguridad informática.
9. Designar a personas no capacitadas para mantener la seguridad, no capacitarlas ni darles tiempo para capacitarse.

Las soluciones a algunos de estos problemas consisten en actividades sencillas, por ejemplo, ubicar la seguridad al mismo nivel jerárquico que otras actividades de la organización, elaborar la misión de la seguridad claramente, promulgar políticas que deriven en la misión o determinar los mecanismos para implementar esas políticas.

Para lograr este último punto, es indispensable considerar cuatro conceptos importantes, que conducirán a una adecuada implementación: misión de seguridad, políticas de seguridad, normatividad y control.

[18] SANS: SysAdmin, Audit, Network, Security Institute. Organización cooperativa de investigación y enseñanza que permite a los administradores de sistemas compartir experiencias y soluciones en seguridad.

[19] Concepto que se definirá en la sección 2.4.4 .

2.2.1 Misión de Seguridad

La Misión define el objetivo principal de una organización, identificando las labores presentes y futuras; para definirla, se debe definir la actividad principal, los problemas que enfrenta y las diferencias con otras organizaciones. Ya que todas las organizaciones son diferentes, no existe una fórmula para redactarla, pero es recomendable que la redacción de la misión se realice en retiros donde participen directivos y empleados, fomentando el intercambio de opiniones y buscando consenso en las propuestas.

Durante la discusión, los participantes más experimentados comparten sus puntos de vista con los inexpertos, lo que garantiza que la misión redactada representa verdaderamente las ideas comunes.

La Misión General debe expresarse en máximo 10 líneas, cuyo texto no debe contener palabras que impliquen obligación como “debe”, “tecnología” o “implementación”; al contrario, debe iniciar a plantearse como buenos deseos: “valores”, “honestidad” o “investigación”. Así mismo, para redactar la Misión de Seguridad, los deseos quedarían definidos como: “disponibilidad”, “integridad” o “confidencialidad”.

Se recomienda que la misión se modifique cada 5 años, replanteando el objetivo de la empresa; para ello se utilizan algunos métodos, como el “Método Delphi”, creado en 1936 por Douglas McGregor, quien observó que las predicciones hechas por un grupo son más acertadas que las que hacen sus miembros individualmente; este método toma las ideas de una comunidad de manera colectiva, estructurando la comunicación de un grupo de personas mientras tratan problemas complejos.

El Método Delphi se aplicó por primera vez en 1948, tratando de mejorar el resultado de apuestas en carreras de caballos; actualmente, además de aplicarse a misiones de seguridad, también puede ser utilizado para determinar la probabilidad de ocurrencia de eventos en un análisis de riesgos, entre otros más.

El Método Delphi se implementa a partir de preguntas estructuradas, dando al grupo las respuestas de todos los participantes para que se consideren de manera individual y anónima.

Una variante de este método es conocida como “Delphi numérico”, el cual tiene prácticamente la misma metodología, a excepción que cada propuesta se evalúa numéricamente de 0 a 10, eliminando las propuestas que tengan menor aceptación, y modificando las restantes hasta obtener, después de varias rondas, un consenso general. Una vez obtenido el texto de la misión se implementan las políticas.

2.2.2 Políticas de Seguridad.

Una política define procedimientos o directrices que deben ser satisfechas, y cambian de acuerdo a los requerimientos de la organización. Por ejemplo, una política de seguridad militar es diferente a una política para una organización comercial o educativa, ya que, la política militar consiste principalmente, en permisos de lectura y escritura, basados en modelos como *Bell y LaPadula*[20].

Para organizaciones comerciales, las políticas pueden implementarse a través de *transacciones correctas* y *separación de funciones*, que se basan en seguimiento de actividades; mientras que, para organizaciones financieras, las políticas se implementan a través del modelo de *Murallas Chinas*, que se basa en relaciones entre organizaciones, es decir, solo se deben mostrar datos que no representen un riesgo a la seguridad de la organización, de acuerdo a los siguientes criterios:

POLÍTICA	CONCEPTO
Militar	Lectura (Confidencialidad) Escritura
Comercial	Transacciones Correctas Separación de Funciones
Financiera	Murallas Chinas (Conflicto de Intereses) (Datos Saneados "sanitized")

Las políticas abarcan diversos ámbitos, como protección y clasificación de recursos, separación de funciones, monitoreo, o buenas prácticas. Para implementarlas, es indispensable realizar un estudio inicial para determinar el estado actual de los sistemas de seguridad; por eso, se deben definir los activos críticos, realizar una evaluación de riesgos, así como usar herramientas empleadas por los atacantes para probar la seguridad de manera real.

La meta al implementar una política es definir las expectativas de la organización en cuanto al buen uso de los recursos, medir la respuesta y prevención de incidentes, y definir sanciones para aquellos que no las respeten.

En seguridad, las políticas son puntos específicos que cubren un área determinada e incluyen las propiedades de confidencialidad, integridad y disponibilidad de acuerdo a la misión de seguridad. Por ejemplo, una política puede abarcar reglas para el adecuado uso de los recursos de cómputo; por lo tanto, las políticas definen responsables y sanciones, a diferencia de la misión, que no contempla a un responsable.

Una política mal elaborada equivale a una vulnerabilidad, lo que deriva en el esquema conocido como “las 4 P’s”, en donde cada organización entra en algún concepto:

[20] Modelo de Seguridad explicado en la sección 2.3.4.

PREMISA	DEFINICIÓN
“Nada está permitido”.	Paranoico
“Lo que no está expresamente permitido, está prohibido”.	Prudente
“Lo que no está expresamente prohibido, está permitido”.	Permisivo
“Todo está permitido”.	Promiscuo

Para que las políticas tengan un seguimiento exitoso, existen herramientas de apoyo que incluyen *Normas* que especifican tecnologías, parámetros o procedimientos, que usados de manera uniforme benefician a la organización y cuyo seguimiento es obligatorio.

Entonces, las *Recomendaciones*, son sugerencias para implementar normas de acuerdo a los requerimientos de la organización; mientras que los *Procedimientos*, son una serie de pasos a seguir para lograr objetivos específicos.

2.2.3 Normatividad.

Las normas son criterios de evaluación que ayudan a clasificar los sistemas de acuerdo a ciertos requisitos y medir el nivel de seguridad que pueden alcanzar. Las normas siguen criterios propuestos en el “Libro Naranja” o criterios normativos modernos conocidos como “Criterios Comunes”. Para realizar la clasificación, la norma exige algunos requerimientos, principalmente en lo relacionado a Políticas, Responsabilidad, Confiabilidad y Documentación. La normatividad se sigue a partir de esquemas como los que propone RFC1244, la norma ISO 7498-2 o los Criterios Comunes, principalmente. La clasificación de los sistemas, de acuerdo a normas, se establece de acuerdo al siguiente cuadro[21]:

	CLASE	CONCEPTO	CARACTERÍSTICAS
Alta Confiabilidad	A2	Implementación verificada	Nivel Experimental. Verificación formal del código fuente, del funcionamiento del hardware, de herramientas de diseño e implementación. Pruebas avanzadas de alto nivel.
	A1	Diseño verificado	Protección verificada, equivalente funcional de B3. Análisis formal y demostración matemática que las políticas y las especificaciones concuerdan. Administración del ciclo de vida.
	B3	Dominios de seguridad	Requiere un monitor de referencia, Administración de Sitio Confiable. Recuperación confiable; es a prueba de ataques.
	B2	Protección estructurada	Kernel de seguridad aislado, protección estructurada, el sistema no se puede penetrar. Modelo formal de las políticas.
Baja Confiabilidad	B1	Etiquetas de seguridad	Protección con etiquetas, todos los objetos “importantes” están etiquetados.
	C2	Protección de control de acceso	Protección por control de acceso, requerimiento de reciclaje de objetos y revisión de documentación.
	C1	Protección voluntaria	Protección voluntaria con seguridad limitada.
	D	Protección mínima	En esta clase se colocan los sistemas que no se han evaluado

[21] Los sistemas B1 o menores son de “baja confiabilidad”; los B2 y mayores son de “alta confiabilidad”.

2.2.4 Control.

El control implica la revisión periódica de las políticas de seguridad implementadas, para evitar una desviación del objetivo principal de la organización.

El control es una actividad a la que se debe dar seguimiento todos los días, no así las demás actividades, que deben cambiar de acuerdo al periodo indicado en el cuadro siguiente:

Concepto	Cambia cada:
Misión	5 años
Políticas	2 años
Normas	6 meses
Controles	diario

2.3 Control de Acceso y sus Políticas.

El control de acceso es un servicio de seguridad que protege los recursos del sistema contra accesos no autorizados, sus antecedentes se remontan a la época prehistórica, cuando el hombre empezó a cazar y a descubrir grandes zonas que no pertenecían a algún grupo. La caza y las luchas por poseer esas tierras originaron conflictos bélicos, por lo que se tuvo la necesidad de construir fortificaciones, y poco a poco, el control de acceso implementado inicialmente por militares, fue adecuándose a la tecnología de cada época. Existen evidencias de que las fortificaciones se construyeron antes que se desarrollara la agricultura, lo que contribuyó al desarrollo de ésta en el interior.

Una de las fortalezas más antiguas data de hace 6000 años y consistía de una valla de troncos rodeada por zanjas, formando un perímetro alrededor de un pueblo; la idea fue evolucionando con la tecnología y las necesidades de la época, como en la muralla china, cuyo longitud abarca miles de kilómetros, aunque nunca pudo completarse.

Otra variante del control de acceso fue la utilización de fosos y bardas exteriores; más tarde, se construyeron empalizadas en la cima de algunas colinas y detrás de fosos de agua, idea que fue utilizada en la construcción de los castillos medievales.

2.3.1 Perímetros.

En la actualidad, las instalaciones físicas se emplean para proteger sistemas de información, con lo que surge el concepto de *Perímetro*, es decir, una barrera física que rodea al sistema de información y lo protege de intrusiones. La entrada es a través de un punto de acceso controlado, por eso se considera que el Control de Acceso va de la mano con la Autenticación, porque en cada entrada se instala una barrera que impide el acceso franco y en la que se realiza la autenticación de quien pretende entrar.

Todos estos elementos forman un Sistema de Control de Acceso, en cuyo perímetro se establecen rondines de vigilancia que verifican la integridad del mismo; en el caso de que ocurra algún incidente, existe un centro de vigilancia externo, capaz de enviar un equipo de respuesta a resolverlo.

Los Sistemas de Control de acceso pueden ser de varios tipos, uno de ellos es el de un sólo perímetro, formado por una sola barrera que divide al exterior y el bien a proteger; aquí se acostumbra implementar autenticación por medio de registro de acceso en una bitácora de entradas y salidas porque el tráfico es intenso; sin embargo, varias personas pueden estar en contacto con el activo, aumentando el riesgo de daño o pérdida.

Como solución, se implementaron los perímetros dobles, es decir, un perímetro dentro de otro perímetro, cuyo antecedente se remonta a construcciones de unos 8000 años de antigüedad y que consisten en una torre dentro de un perímetro interior. Ahí se refugiaban las personas importantes y se resguardaban los valores y provisiones. En la actualidad, estos esquemas permiten aislar el bien a resguardar, ya que existen dos barreras que lo separan del resto del mundo, reduciendo el número de personas en su entorno inmediato y simplificando la vigilancia directa y la obediencia; en caso de incidente, la respuesta es más sencilla porque es más fácil robustecer el segundo perímetro.

En sistemas que requieren mayor seguridad, se implementa un triple perímetro, que consiste en listas de acceso y análisis de bitácoras (adicionales a las que se encuentran en el primer perímetro); en caso de incidente, es posible tener respuesta inmediata porque el tráfico es mínimo, el mundo exterior es muy distante, y la supervisión se concentra en un punto crítico; lo que simplifica la autenticación y el reforzamiento del tercer perímetro.

2.3.2 Autenticación

Los antecedentes históricos de la Autenticación pueden apreciarse en las pinturas rupestres que muestran a un grupo de guerreros uniformados siguiendo a su líder, éste porta un uniforme más vistoso para distinguirse de sus tropas.

Ello demuestra que es difícil reconocer a una persona entre un grupo, lo que derivó en la implementación de los uniformes; aunque si el enemigo se hacía de uno, podía violar la seguridad; esto provocó la implementación de otra metodología llamada “santo y seña” que era complemento del uniforme; esta metodología persiste hasta hoy en actividades militares; de su estricto cumplimiento depende la seguridad de las tropas y del equipo.

La implementación de Perímetros, junto con Autenticación, dieron origen a lo que hoy se conoce como *Políticas de Control de Acceso*; con ellas, se puede acotar el sistema por medio de un inventario de activos, es decir, el registro de los elementos del sistema: componentes lógicos y físicos, usuarios y administradores.

A partir de este conocimiento se pueden implementar políticas de seguridad, ya que en cada interacción es posible identificar y autenticar las partes involucradas. El sistema se considera acotado a los elementos registrados en el inventario; por definición, los elementos que no aparezcan, no forman parte del sistema. Sin embargo, el inventario es modificable a lo largo del tiempo, incluyendo altas, bajas y cambios.

Así, el control de acceso incluye tres procesos: el registro de componentes del sistema, la identificación de los mismos y su autenticación. Es importante notar que los sistemas de información comparten requerimientos de cualquier otro sistema acotado.

A manera de ejemplo, se puede pensar en el proceso de inscripciones escolares, donde cada alumno acude a inscribirse en las oficinas de servicios escolares del plantel (proceso de registro). El proceso de identificación se realiza por medio de un documento, que puede ser el acta de nacimiento o algún otro documento emitido por alguna entidad gubernamental.

Cuando terminan estos dos procesos, la escuela deberá emitir una credencial o tira de materias, que permitirá autenticar al alumno cada vez que requiera hacer uso del sistema, es decir, de los servicios que ofrece la escuela (proceso de autenticación). El sistema está acotado a los alumnos del plantel, quienes se pueden dar de alta, de baja o cambiar su situación escolar; así mismo, la escuela podrá compartir información con otros planteles y entidades.

2.3.3 Autenticadores.

En la actualidad, para realizar la autenticación de usuarios, se emplean diversos mecanismos, que se clasifican en cuatro grupos de acuerdo a sus características; la seguridad aumenta al usar autenticadores de grupos distintos. Así, al momento de registrar a un usuario, se le solicita depositar (o se le asignan) varios de los autenticadores descritos a continuación, que deberá exhibir cuando se requiera:

Autenticadores Basados en Conocimiento.

Se basan en algo que el usuario conoce y consisten en un secreto compartido entre el usuario y el sistema de información; generalmente es una contraseña formada por caracteres alfanuméricos que el usuario muestra para ingresar al sistema.

Por ser un secreto compartido, se debe proteger tanto en el registro en el sistema, del lado del usuario, y durante la trayectoria entre ambos; si existe una protección deficiente en cualquiera de estos puntos, se puede hacer mal uso de ese secreto. Aunque el punto débil casi siempre resulta ser el usuario, quien divulga sus contraseñas a los compañeros; la mejor solución a este problema es la capacitación y la concientización.

Autenticadores Basados en Posesión.

Se realiza por medio de un dispositivo y se basa en algo que el usuario tiene, como una tarjeta inteligente con procesador y memoria. Existen diferentes formas de operación de estas tarjetas, por ejemplo, cifrar la contraseña del usuario y transmitirla inmediata o posteriormente; otra opción es que el dispositivo genere contraseñas con cierta frecuencia, de manera sincronizada con el sistema al que permite acceso, compartiendo el secreto. También pueden usarse protocolos de tipo “santo y seña digitales" en los que el dispositivo y el sistema intercambian "preguntas" y "respuestas" predeterminadas algorítmicamente.

Autenticadores Basados en Características del Usuario.

Este método es conocido también como “Autenticación Biométrica” y consiste en el uso automatizado de características de una persona para verificar su identidad. La Biometría[22] considera las características físicas del cuerpo que no se alteren fácilmente, visibles con el atuendo normal de las personas y que puedan expresarse matemáticamente.

Para realizar la autenticación, un dispositivo recolecta las características que deposita el usuario al momento del registro, realiza su descripción matemática y las guarda en una lista de usuarios.

[22] Nombre con el que también es conocida la autenticación biométrica.

Al solicitar acceso, el usuario exhibe la característica que haya registrado, el sistema recalcula la descripción matemática y la compara con la que se encuentra almacenada. La biometría puede ser fisiológica, si se basa en medidas de partes del cuerpo (los dedos, el iris, la retina, la mano o el rostro), o conductual, si se basa en la medida de las acciones de una persona (la voz, el uso de un teclado y la firma).

La principal característica de los sistemas biométricos es su precisión, aunque existe un porcentaje de usuarios válidos que son rechazados por error (rechazos falsos), a estas fallas se les conoce como “Errores de Tipo I”. Por su parte, el porcentaje de impostores que son aceptados (aceptaciones equivocadas) se le llama “Errores de Tipo II”, y representan los errores más graves, pues permiten el acceso de intrusos o suplantadores.

Por ello, todos los sistemas biométricos permiten ajustar algunos parámetros para eliminar las aceptaciones falsas y optimizar su funcionamiento, logrando una tasa de aceptaciones falsas de cero. Además, para eliminar los rechazos falsos, el sistema se puede ajustar para permitir el acceso con una verificación aproximada. Debido a la precisión de estos sistemas y sus diferencias en rapidez, es necesario combinar varias tecnologías.

Autenticadores Basados en Posición.
Método de autenticación también conocido como “geoposición”, y que está basado en algo que determina la posición sobre la Tierra; consiste en leer las señales de los satélites de geoposicionamiento por medio de un aparato llamado “Cyberlocator”; estas señales son transformadas en una “firma de ubicación” (location signature), que incluye la hora en que se hicieron las observaciones.

Desde cualquier punto de la Tierra se pueden recibir señales de la red de geoposicionamiento[23], la cual identifica el lugar y el momento en que un dispositivo estuvo en cierto lugar, lo que permite rastrear la conexión a Internet; además, si se incluye la firma de ubicación en un documento, se puede asegurar dónde y cuándo se creó, evitando que un usuario legítimo se lleve información a un destino inapropiado.

2.3.4 Esquemas de Control de Acceso.

En la actualidad existen diversos esquemas del control de acceso, cada uno apropiado para ciertas condiciones, considerando el nivel de seguridad y el valor del bien a asegurar.

Control de Acceso Discrecional.
Este esquema considera al usuario (sujeto) como dueño del archivo, programa o dispositivo que adquiere (objeto); por ello, es el único que puede asignar (o negar) derechos a otros usuarios sobre el archivo. Este esquema se implementa mediante técnicas como “bits de permiso”, “sistemas de contraseñas”, “listas de capacidades” o “listas de control de acceso”.

Los sujetos también son objetos pues pueden recibir las consecuencias de las acciones de otros sujetos, como Leer (R), Escribir (W), Añadir (A), Ejecutar (E) y Poseer (O).

[23] Red implementada por el gobierno de los Estados Unidos.

De esta manera, en el elemento de la matriz que corresponde a un sujeto y a un objeto se colocan los derechos que le otorgan las políticas de seguridad; si un elemento de la matriz aparece en blanco, ese sujeto no tiene ningún derecho sobre el objeto, como se muestra:

	Segmento1	Segmento 2	Archivo 1	Archivo 2	Proceso 1
Juan	**RW**		**A**		**E**
María				**RWE**	
Proceso 1		**A**			

En la matriz, el sujeto “Juan” tiene derechos de lectura (R) y escritura (W) sobre el objeto “Segmento 1”; de la misma forma, el sujeto “María” tiene derechos de lectura (R), escritura (W) y ejecución sobre el objeto “Archivo 2”, sin embargo, el mismo sujeto “María” no tiene derechos sobre el objeto “Archivo 1”.

Así, cuando un sujeto solicita actuar sobre un objeto, una parte del sistema operativo, conocida como *Monitor de Referencia*, adquiere los identificadores de ambos, realiza la autenticación correspondiente y permite la acción solicitada. Para cambiar el estado de un sistema se emplea un conjunto de comandos basados en seis operaciones primitivas, como: *coloca* el derecho *r* en *A*, *borra* el derecho *r* en *A*, *crea* el sujeto, *crea* el objeto, *destruye* el sujeto, y *destruye* el objeto.

Dentro de un programa, la protección se modela con una matriz más refinada, donde los sujetos y los objetos son procedimientos, y los derechos sobre un objeto de datos quedan determinados por las operaciones y procedimientos que se le pueden aplicar. Sin embargo, este esquema se puede atacar mediante “caballos de Troya”, que ocultamente copian al directorio de otro usuario todos los archivos sobre los que tiene control, otorgando permisos ilimitados al segundo usuario.

Control de Acceso Obligatorio.
En este esquema, el usuario recibe un *Nivel de Autorización de Acceso* y la información se clasifica según su sensibilidad; luego, estos dos parámetros se combinan para crear *Clases de Acceso*. El esquema también considera a un Objeto como cualquier ente pasivo que contiene información (por ejemplo, un archivo), y a un Sujeto como cualquier ente activo que funciona en nombre de los usuarios (como puede ser un Proceso).

De esta manera, se logra que cada sujeto y cada objeto tengan una etiqueta; la autorización de acceso se basa en comparar la etiqueta del objeto con la etiqueta de sujeto mediante el operador de dominancia “>”. Así, “A > B” indica que la etiqueta A domina a la etiqueta B, por lo que, se pueden definir operaciones permitidas o prohibidas que reflejan las políticas de seguridad. Existen varios modelos que utilizan el control de acceso obligatorio, los cuales se detallan a continuación:

- **Modelo de Bell y LaPadula**

Es uno de los esquemas de control de acceso obligatorio más usados y antiguos; consiste en colocar etiquetas en los sujetos y objetos, con el fin de proteger principalmente la confidencialidad, de acuerdo al siguiente esquema:

Donde:

S = conjunto de todos los sujetos en un sistema
O = conjunto de todos los objetos en un sistema

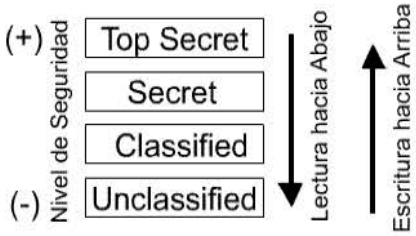


Fig 2.4. Modelo Bell Lapadula

Para cada sujeto *s* en *S* existe una clase de acceso C(*s*) Para cada objeto *o* en *O* existe una clase de acceso C(*o*)

Así, un sujeto *s* puede leer un objeto *o* solo si: C(*s*) >C(*o*)
Un sujeto *s* puede escribir en un objeto *o* solo si: C(*s*) < C(*o*)

Explícitamente, no se puede leer de niveles arriba, si se permitiera, alguien con una clasificación de confidencialidad más baja podría acceder a información etiquetada con clasificación alta, perdiendo la confidencialidad. Tampoco se puede escribir niveles hacia abajo, si se permitiera, alguien con una clasificación de confidencialidad alta podría colocar información altamente confidencial en un archivo de baja confidencialidad (fig. 2.4).

Así, un sujeto puede leer y escribir un objeto si ambos tienen la misma clase de acceso. De hecho, este modelo limita severamente el trabajo diario de una organización, ya que no será posible intercambiar información entre sujetos de niveles distintos.

Sin embargo, esta ineficiencia se puede evitar, haciendo que el usuario de mayor jerarquía inicie una sesión de jerarquía inferior, durante la cual su jerarquía se ve degradada. Así mismo, para que un usuario pueda escribir en archivos de clase menor a la suya, se deben implementar sesiones que tengan una clase de acceso adecuada.

Este modelo también se aplica al control de acceso físico, estableciendo una jerarquía de confidencialidad y asignando una clase a cada persona, luego, se establece una jerarquía de confidencialidad de los sitios. Basta indicar la jerarquía de confianza para que la persona acceda al lugar al que tiene derecho, y registrar a los nuevos usuarios en el acervo central de autenticación (que puede ser incluso mundial). Así, no hay que actualizar listas de control de acceso.

A pesar de sus ventajas, este modelo presenta algunas vulnerabilidades conocidas como “canales encubiertos”, que son trayectorias que se pueden usar para violar el control de acceso debido a un error en la implementación de la política de seguridad, permitiendo el flujo de arriba hacia abajo en la jerarquía de confidencialidad. Este ataque consiste en dos programas, uno es un Caballo de Troya, que se coloca en el extremo alto de la jerarquía, el otro programa se coloca en el extremo más bajo.

Existen diversos tipos de canales encubiertos; uno de ellos es conocido como “canal de almacenamiento”, que emplea recursos compartidos por sujetos de distintas clases. También existen “canales de Sincronía”, que emplean mecanismos que permiten a un sujeto afectar el funcionamiento de otro sujeto de menor jerarquía. Un método de defensa consiste en evitar que se compartan recursos, así como crear una partición del disco para cada clase de acceso.

- **Modelo de BIBA**

Este modelo está enfocado a proteger la integridad de la información por medio de la restricción de accesos de lectura y escritura; se utiliza principalmente en organizaciones no militares donde es más importante la integridad que la confidencialidad. Este modelo considera que la integridad de los datos consiste en evitar la modificación no autorizada.

La integridad de un programa consiste en que el sistema proporcione dominios de ejecución protegidos, mientras que la integridad de un usuario consiste de su propio cuidado y responsabilidad.

Entonces, un archivo de alta integridad es aquel que ha sido creado por un proceso de alta integridad. Es decir, sea *S* el conjunto de todos los sujetos en un sistema y *O* el conjunto de todos los objetos, se considera que cada sujeto *s* en *S* y cada objeto *o* en *O* tienen una clase de integridad I(*s*) y I(*o*), por lo tanto, un sujeto *s* puede modificar un objeto *o* sólo si I(*s*)>I(*o*); también, un sujeto *s* puede leer un objeto *o* sólo si I(*o*)>I(*s*).

El modelo consiste en que no se puede escribir hacia arriba para evitar que un usuario de baja integridad degrade información de alta integridad; tampoco se puede leer de abajo para no contaminar información de alta integridad con información de baja integridad. Un sujeto puede leer y escribir un objeto sólo si tienen la misma clase de integridad (fig. 2.5).

Se puede combinar el modelo *Bell LaPadula* con el modelo de *Biba* para mantener la confidencialidad y la integridad de la información, esto se logra empleando jerarquías de confidencialidad o integridad. Así, surge el concepto de “compartimiento”, que consiste en dos conjuntos, en los que el dominio se establece si uno es subconjunto de otro; también es posible que dos conjuntos no tengan relación de dominio.

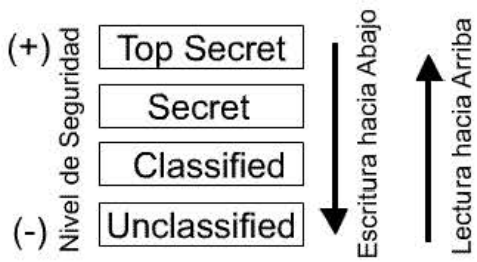


Fig 2.5. Modelo Biba

Los compartimientos sirven para implementar políticas de tipo “requerimiento de conocimiento”, es decir, además de ejercerse un control de acceso jerárquico, se puede aplicar la regla de otorgar el mínimo conocimiento a un sujeto para que lleve a cabo su función, independientemente de su jerarquía.

- **Modelo de Clark y Wilson**

Este modelo se basa en dos mecanismos a implementar, las "Transacciones Bien Formadas" y la "Separación de Funciones", en las que los datos pueden ser "Controlados" o "No Controlados", y en donde además, los sujetos pueden transformar los datos mediante "Procedimientos Transaccionales", es decir, procedimientos que llevan de un estado válido a otro. Así, Clark y Wilson emitieron su modelo basado en algunas reglas sencillas y considerando todas las entidades anteriores.

Control de Acceso Basado en Roles.

Este esquema otorga permiso a los roles o perfiles para cada usuario, registrando al usuario bajo el rol apropiado. Así, no es necesario que los permisos se otorguen persona a persona, simplificando la administración de los permisos y ofreciendo más flexibilidad para especificar y vigilar la obediencia de las políticas. Este método reconoce que el dueño de la información es la organización, por lo tanto, no es un método discrecional, pero tampoco es un método obligatorio.

El método permite que un usuario asignado a un perfil con privilegios mayores tenga acceso a información sensible, mientras que un usuario asignado a un perfil con menos privilegios, sólo pueda consultar parte de la información; de hecho, se pueden combinar los métodos anteriores para mejorar la administración de la seguridad y de las políticas.

En entornos que requieren mantener la confidencialidad se emplean perfiles para implantar el modelo de Bell y LaPadula, mientras que en sistemas distribuidos se establecen dominios de protección globales y locales; también puede haber perfiles dentro de otro perfil general, por ello, este modelo se implementa basado en reglas.

Control de Acceso Optimista.

Cuando se trabaja en un entorno de transacciones dinámicas pueden ocurrir eventos críticos, que no pueden ser corregidos por el personal a cargo debido a la falta de privilegios. Este esquema de seguridad permite relajar las políticas para corregir algún desperfecto, basándose en la buena fe de los usuarios y de los administradores, ya que la obediencia a las reglas es retrospectiva.

Las violaciones a los controles de seguridad se permiten solo si son auditados minuciosamente y si ofrecen la posibilidad de ser corregidos apropiadamente; de esta manera, el control se basa en la posibilidad de deshacer las consecuencias de las violaciones, de efectuar acciones punitivas en caso de que fueran necesarias (despidos o acusaciones judiciales), y en la revocación de privilegios.

Se supone que el costo de todo lo anterior es más bajo comparado con las consecuencias de una negación de acceso en caso de emergencia y para realizarlo exitosamente, se establecen listas de autorizaciones usadas en circunstancias extraordinarias, excepto en accesos que puedan resultar en fallas catastróficas o daños irreversibles. Además, existen requerimientos que permiten regresar al sistema a su estado original, como los *Puntos de Acceso Restringidos*, la *Responsabilización* y la *Auditoria* mediante bitácoras.

2.4 Seguridad en Redes y en Internet

En el capitulo 1 de este trabajo, se mencionaron algunos de los conceptos importantes del funcionamiento de las redes, así como algunos de sus principales problemas de seguridad. Una vez cubiertos los conceptos básicos, esta sección se enfoca hacia el funcionamiento de las redes e Internet, a describir sus principales problemas y a proponer algunas posibles soluciones a los mismos.

Así, se define a una *Red de Computadoras* como un conjunto de computadoras autónomas, interconectadas entre sí de formas muy variadas; sus objetivos son compartir recursos, realizar la transferencia de información y la comunicación entre los equipos conectados. Las redes utilizan, generalmente, medios de transmisión públicos, por ello, tanto los recursos y como la información están expuestos a ataques.

2.4.1 Modelo de Referencia OSI

La base actual de funcionamiento de las redes de computadoras es el "Modelo OSI[24]", que consta de siete capas, donde cada una depende de los servicios proporcionados por la capa inferior. Las capas equivalentes realizan funciones similares, por ello existe correspondencia entre las capas OSI del emisor y del receptor; así, se describen las comunicaciones en las redes de computadoras.

Las funciones de cada capa se describen a continuación en la (fig 2.6):

	CAPA	RESPONSABILIDAD	ACCIÓN
7	Aplicación	Programa de Usuario	Inicia mensaje; cifrado opcional.
6	Presentación	Utilerías del Sistema	Divide el mensaje en bloques, compresión de texto, cifrado opcional.
5	Sesión	Sistema Operativo	Establece una sesión de usuario a usuario; encabezado agregado para mostrar emisor, receptor y secuencia de información.
4	Transporte	Administrador de Transporte	Control de flujo, prioridad del servicio, información agregada referente a la conexión lógica.
3	Red	Administrador de Red	Ruteo, bloqueo de mensajes en paquetes, información de ruteo agregadas a bloques.
2	Enlace de Datos	Hardware	Recuperación de errores en la transmisión, separación del mensaje en *frames*; encabezado y rastreador agregado a secuencia y detectores de errores.
1	Física	Hardware	Transmisión física de señales por bits individuales.

Fig 2.6. Capas del Modelo OSI.

Cualquier red puede construirse usando los mismos protocolos que utiliza Internet (Fig. 2.7) ya que Internet en realidad es una red de redes que funciona a través de backbones, es decir, una columna principal que sirve como conexión a las demás redes.

[24] OSI: Open System Interconection. Sistema de Interconexión Abierto.

Las comunicaciones a través de Internet funcionan a través de host, es decir, se conecta un host a una red LAN, que a su vez está conectada al backbone de la organización, luego, ese backbone se conecta al backbone del ISP, y por último el ISP se conecta al backbone de Internet. Para usar un servicio de cierto host, se debe indicar al navegador y conectarlo a ese host.

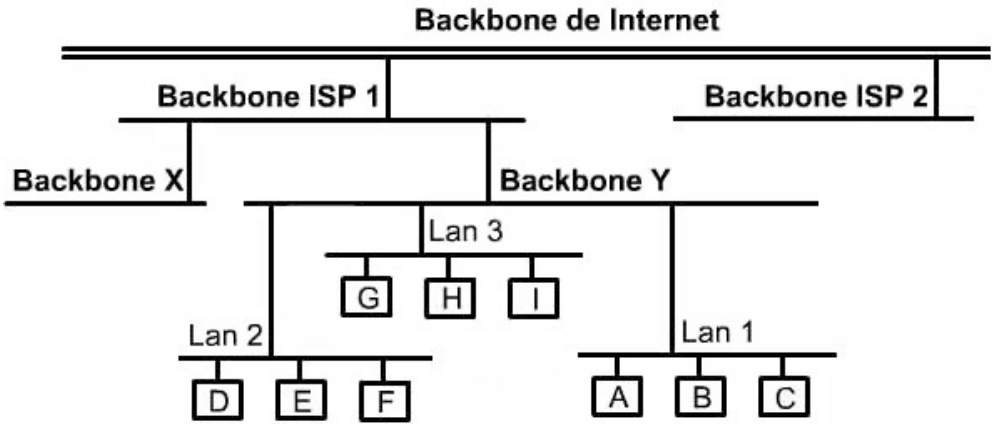


Fig 2.7. Diagrama de Backbone de Internet.

Esto se logra enviando paquetes (datagramas) a través de la plataforma de servicios y protocolos al ISP, y luego a una red donde están conectados, y así, hasta el backbone del host que provee el servicio, y por último, hasta el host solicitado. Cuando la petición llega al host, éste responde enviando paquetes pero ahora en sentido contrario.

Internet se forma por hosts distintos entre sí en hardware y software; para la comunicación se usa el conjunto de protocolos TCP/IP[25]. Investigadores de todo el mundo participan en el grupo de trabajo IETF[26] diseñando los protocolos para Internet: IP ("Internet Protocol"), TCP ("Transport Control Protocol"), UDP ("User Datagram Protocol"), ICMP ("Internet Control Message Protocol"), y otros más; cada uno opera en una capa específica del modelo OSI, como se muestra en la (Fig. 2.8).

Modelo de Referencia OSI	Protocolo de Internet	
Aplicación	FTP, Telnet SMTP, SNMP	NFS XDR RPC
Presentación		
Sesión		
Transporte	TCP, UDP	
Red	Protocolos de Ruteo	IP
Enlace	ARP, RARP	
Física	No Especificado	

Fig 2.8. Protocolos de Internet.

[25] "Transfer Control Protocol/Internet Protocol", protocolo abierto que cualquiera puede implementar libremente y que sirve como "lenguaje" de Internet

[26] Internet Engineering Task Force. Fuerza de Tarea para Internet, que diseña los protocolos para Internet.

IP (Internet Protocol)
Es el más importante de los protocolos de Internet y trabaja en la capa 3 (capa de Red) del Modelo OSI; se encarga, entre otras funciones, de transportar datagramas, mapear direcciones de Internet (como 132.248.10.7) a una dirección física de red (como 08:00:69:oa:ca:8f), y realizar el ruteo para que los dispositivos que se conectan a Internet sigan la ruta correcta.

Desde el punto de vista de la comunicación, IP tiene características que lo hacen robusto y flexible, pero desde el punto de vista de seguridad, carece de elementos para funcionar confiablemente, ya que lleva a hoyos de seguridad que pueden ser usados para engañar sistemas, permitiendo conexiones desde sistemas que no debería ser permitida su conexión y facilitando el trabajo a los intrusos.

Por otro lado, IP no ejecuta un mecanismo de autenticación fuerte, es decir, no comprueba que el origen de un paquete sea válido; por eso, la autenticación tiene que darse en las capas superiores; así, aplicaciones que requieren autenticación del host, como las aplicaciones criptográficas, lo hacen en la capa 7 (Capa de Aplicación).

Algunos ataques sobre IP son bien conocidos; como “IP Hijacking”, un ataque relativamente sofisticado pero muy dañino, que consiste en que la sesión del usuario es tomada bajo el control del atacante; así, éste puede ejecutar cualquier comando y ver información como si fuera el usuario atacado. Por ejemplo, si el usuario esta utilizando el correo electrónico, después del ataque verá que su sesión termina, y procederá a conectarse otra vez sin notar que el atacante está realizando acciones en su nombre. Existen en el “inframundo”[27] herramientas que permiten realizar este ataque.

Existe además un ataque a IP conocido como “DoS”[28], y consiste en realizar más peticiones de servicio que las que un equipo de cómputo puede atender, de esta forma, al saturar el servicio llegará un momento en que se venga abajo. El ataque DoS es muy fácil de realizar pero muy difícil (casi imposible) de seguir, ya que no es fácil rechazar una petición del atacante sin rechazar también los requerimientos legítimos de servicio.

Existen herramientas en el “inframundo” que simplifican la realización del ataque Dos, donde el programa del atacante hace una conexión a algún puerto de servicio y satura la conexión. Para evitarlo, se usa filtrado de paquetes, es decir, se verifican los paquetes que entran a la red para evitar su falsificación. Otro ataque conocido a IP es “IP Spoofing” [29].

TCP (Transport Control Protocol)
Es un protocolo de Capa 4 (capa de transporte), diseñado precisamente para transportar paquetes TCP, garantizando su entrega; es decir, si el host *A* envía paquetes al host *B*, *A* espera la confirmación de recepción, si *B* no envía confirmación en un tiempo específico, entonces *A* reenvía el paquete.; las aplicaciones en el host *B* deben esperar el flujo de datos completo para efectuar la aplicación.

[27] Se conoce así al mundo de los hackers, donde se pueden encontrar programas o herramientas piratas.
[28] DoS. Deny of Service o Negación de Servicio
[29] Este concepto se explica ampliamente en el capítulo 3 de este trabajo, bajo el título de “Pharming”

Si un paquete se pierde, será reenviado por A, y si los paquetes llegan en desorden, B los reordena antes de pasar los datos a la aplicación. Así, TCP ordena secuencialmente los paquetes, realiza la corrección de errores e implementa conexiones entre hosts.

TCP e IP se diseñaron para operar juntos, y colectivamente se conocen como TCP/IP; a través de estos protocolos pueden implementarse varios servicios, como telnet, ftp, rlogin y SMTP, orientados a conexión y con requerimientos de confiabilidad altos. Por ejemplo, un servidor DNS usa TCP (en algunos casos) para transmitir y recibir nombres de dominio, pero emplea UDP para transmisión de información acerca de anfitriones individuales.

Sin embargo, existen errores de TCP/IP que son factor para no lograr seguridad, aunado a esto, no se cuenta con control, legislación y administración a nivel mundial, lo que fomenta cada vez mayor cantidad de ataques y fraudes a través de Internet.

IPSec

En 1994, debido a los problemas con TCP/IP, el *Internet Architecture Board* [30] emitió un reporte titulado "*Seguridad en la Arquitectura de Internet"* (RFC 1636), en el que se identifican áreas clave para los mecanismos de seguridad, como el aseguramiento de la red contra monitoreo no autorizado, control de tráfico, así como el uso de autenticación y mecanismos de cifrado.

El IAB incluyó a la autenticación y la integridad como características de seguridad necesarias para funcionar con IP; así surge la nueva generación de IP conocida como IPv6[31] cuyas características pueden utilizarse actualmente ya que funcionan para IPv4 e IPv6. Entonces, la seguridad al nivel IP comprende tres áreas funcionales: autenticación, confidencialidad y administración de llaves.

Así, IPSec proporciona la capacidad de asegurar las comunicaciones a través de una LAN, de redes privadas y públicas WAN, e Internet. IPSec es transparente a las aplicaciones debido a que reside debajo de la capa de transporte (TCP, UDP), como se muestra (fig. 2.9).

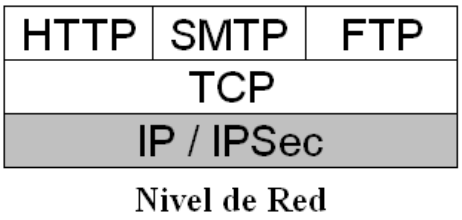


Fig 2.9. IPSec trabajando debajo de TCP

Cuando se implementa IPSec en un firewall o un ruteador, proporciona seguridad fuerte a todo el tráfico que cruza el perímetro, además, es transparente para los usuarios, por lo que no se requiere entrenamiento sobre los mecanismos de seguridad. IPSec brinda también servicios de seguridad en la capa IP[32] y permite al sistema elegir los protocolos de seguridad, determinar los algoritmos a usar para los servicios y establecer la llave criptográfica para ellos.

[30] IAB por sus siglas en inglés, es un Cuerpo asesor de Internet Society (ISOC) , y a su vez, comité que forma parte de Internet Engineering Task Force (IETF).

[31] IP Versión 6

[32] Servicios como Control de Acceso, Integridad sin conexión, Autenticación de origen de datos, Rechazo de paquetes replicados y Confidencialidad.

Para que estos servicios funcionen adecuadamente se necesitan dos protocolos: el protocolo de autenticación, llamado *"Authentication Header" (AH)*; y un protocolo que combina cifrado y autenticación, llamado *"Encapsulating Security Payload" (ESP)*. Ambos protocolos soportan dos modos de uso, el primero es conocido como "Transporte", que brinda protección para protocolos de capas superiores; el segundo es conocido como "Túnel", que proporciona protección al paquete IP completo.

La comunidad de Internet ha desarrollado mecanismos de seguridad para aplicaciones específicas en diferentes ámbitos, tales como S/MIME y PGP para correo electrónico, Kerberos para autenticación en modelos cliente servidor, SSL para Web, entre otras.

2.4.2 Aplicaciones Criptográficas.

La criptografía moderna ha tenido grandes avances, principalmente en sus aplicaciones, que sirven de base a la seguridad actual; entre los más importantes están los siguientes:

Protocolos criptográficos.

Para entender a la criptografía y sus aplicaciones, se debe definir lo que es un protocolo, base para la implementación de la seguridad.

Un Protocolo es un acuerdo entre dos o más partes para realizar una tarea específica; consiste en una serie de pasos bien definidos que producen un resultado. Durante el proceso todos las partes conocen el protocolo, están de acuerdo en seguirlo y saben claramente lo que cada parte gana con su ejecución.

Existen tres tipos de protocolos; el primero de ellos es conocido como *"Protocolo Arbitrado"*, basado en una tercera parte confiable (árbitro o juez), quien no tiene ninguna preferencia por alguna de las partes. Este protocolo resulta poco práctico por la dificultad de tener una tercera parte confiable y neutral.

El segundo tipo es llamado *"Protocolo Adjudicado"*, y es una variante del protocolo arbitrado porque se basa en una tercera parte confiable, la cual, no siempre es requerida, ya que si todas las partes respetan el protocolo, el resultado se logra sin ayuda de un juez.

Por último, el *"Protocolo Autoimplementado"*, es considerado como el mejor protocolo, ya que está diseñado para hacer imposible el engaño. No requieren árbitro, ya que por sí solos garantizan que si un participante en el protocolo trata de engañar, sea descubierto por los otros participantes inmediatamente.

Firmas Digitales

La firma representa un rasgo distintivo de la identidad del firmante, ya que es infalsificable (nadie más puede reproducir dicha firma), no reusable (una firma no puede utilizarse en varios documentos), inalterable (si una firma se altera, pierde su validez) y no repudiable (quien firma, no puede negar haber realizado tal acto). Así, la Firma Digital se basa en las características de la firma autógrafa, por tanto se considera que es una transformación de la firma autógrafa al mundo digital, porque relaciona de forma única al documento a firmar, a la función de firma y a la llave de firma (elemento propio de la identidad del firmante).

La Firma Digital consiste en dos procesos: el Proceso de Firma y el Proceso de Verificación de Firma.

El Proceso de Firma inicia cuando, aplicada la transformación de firma al documento (usando la llave privada del firmante), se produce la firma digital, que se envía al destinatario junto con el documento firmado.

Por su parte, el Proceso de Verificación de Firma lo realiza el receptor aplicando una función de verificación por medio de la llave de verificación (llave pública o de verificación de firma); el resultado arroja uno de dos posibles valores: verdadero ó falso; por lo tanto, si la verificación es válida, la firma se acepta; de lo contrario, se rechaza.

Si un documento requiere ser firmado digitalmente por varias personas (firmas múltiples), se utiliza un protocolo arbitrado (tercera parte confiable), que actúe como juez y que verifique las firmas de cada uno de los firmantes. De este modo, combinando la firma digital con criptografía de llave pública se obtiene la seguridad del cifrado, la autenticidad de la firma, no repudio y confidencialidad. Algunos algoritmos que implementan los servicios de firma digital son Elgamal, DSS[33] y DSA[34].

Certificados Digitales.

Un Certificado Digital (CD) es un documento público verificable que contiene información acerca de su propietario, ya sean personas, organizaciones, dispositivos de hardware, o procesos de software; es emitido por una Autoridad Certificadora (AC) y sirve como un identificador para transacciones electrónicas.

Un CD se considera infalsificable porque los mecanismos usados para su generación garantizan que sólo una AC pudo emitirlo; por ejemplo, la AC incorpora su firma digital al CD; además, si el certificado es modificado, su valor hash cambia y no coincide con la firma que la AC generó para él; ambos elementos lo convierten en infalsificable.

Un CD contiene información referente a la llave pública del dueño, nombre, fecha de expiración, nombre de la AC que generó el certificado, número de serie y firma digital del emisor (fig. 2.9). Así, el CD garantiza que la llave pública pertenece a la entidad certificada y que dicha entidad posee la correspondiente llave privada; con ello, se implementan los servicios de Identificación, Autenticidad y No repudio.

Por su parte, la AC es una organización confiable que acepta solicitudes de certificación, emite certificados, mantiene información de ellos y brinda servicios para el uso de los certificados que emite. Para que un CD sea emitido, el usuario debe generar su par de llaves (pública y privada) y almacenar la llave privada de forma segura (cifrada); luego, debe solicitar el certificado y enviar sus datos y la llave pública a la AC; por último, la AC comprueba la información proporcionada por el solicitante.

[33] Digital Signature Standard
[34] Digital Signature Algoritm

De acuerdo a la entidad a la que están emitidos, los certificados se dividen en clases: Las clases 1 y 2 se emiten a personas, y se utilizan en compras y suscripciones en línea; para emitirlos, la AC no realiza verificación de los datos del solicitante, a excepción de su nombre, dirección y algún otro.

Los CD Clase 3 y 4 son emitidos sólo a organizaciones, previa validación de su identidad y el cumplimiento de estándares financieros.

Una vez validados los datos, la AC genera el certificado y lo firma con su llave privada, luego distribuye los certificados por diversos mecanismos: servidores, directorios y correo electrónico, lo que permite que una entidad busque el certificado de otra, lo instale en una aplicación de correo electrónico y lo use para enviar correo seguro; también se usan para intercambiar o distribuir llaves en comunidades grandes.

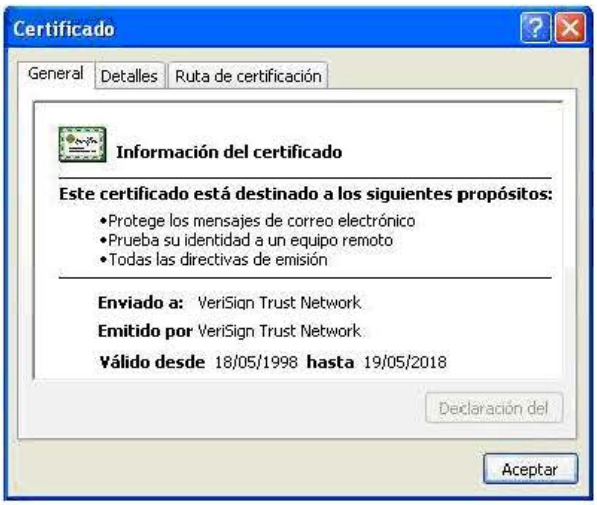


Fig 2.10. Certificado Digital

Criptoanálisis.

El criptoanálisis es la contraparte de la criptografía, ya que es la ciencia que busca descifrar un mensaje cifrado sin poseer la llave correspondiente, para ello, utiliza diversas técnicas como el ataque por “Fuerza Bruta”, que consiste en probar todo el conjunto posible de llaves hasta encontrar aquella que descubra el texto cifrado; millones de llaves son probadas sucesiva (o simultáneamente) intentando descifrar el mensaje y asumiendo que el atacante conoce el algoritmo de descifrado.

En general, un ataque por fuerza bruta puede durar, en promedio, la mitad del número posible de llaves multiplicado por el tiempo para probar cada llave. En la práctica, la seguridad de un criptosistema sólo puede ser medida a por el número de intentos por romperlo; aquellos sistemas que han resistido numerosos ataques se consideran seguros, por ello, recientemente han sido inventadas nuevas y mejores técnicas de criptoanálisis.

Por otro lado, los algoritmos son seguros cuando se usan apropiadamente, por esta razón, los ataques se dirigen a los protocolos. Algunas aplicaciones de la criptografía son implementadas a través de software, como los descritos en la siguiente sección.

Pretty Good Privacy (PGP)

Es un software desarrollado en 1991 por Phillip R. Zimmermann, que permite intercambiar mensajes, asegurar archivos (y discos completos) mediante cifrado, y realizar conexiones de red con la certeza de que la comunicación y almacenamiento de información es confidencial y con autenticación fuerte.

Para que PGP pudiera desarrollarse, Zimmermann tuvo que sortear algunos procesos legales iniciados, por una parte, por el Gobierno de los Estados Unidos a través de ITAR[35], que buscaba evitar que PGP pudiera ser exportado fuera de ese país; y por otro lado, por la compañía RSA, dueña de los derechos de RSA, base de los algoritmos utilizados en el desarrollo de PGP. Para evitar estos problemas, Zimmermann firmó un acuerdo con el Massachusetts Institute of Technology (MIT), dueño de parte de los derechos de RSA, y utilizó otras bibliotecas, en versiones posteriores de PGP.

Los elementos principales de PGP se dividen de acuerdo a su funcionalidad, es decir, las Firmas digitales, el Cifrado, la Compresión de Datos, el proceso de Conversión Radix-64, la Segmentación y la Administración de llaves. La relación de estos elementos conforman los dos servicios de seguridad implementados por PGP: confidencialidad y autenticación.

PGP implementa confidencialidad usando criptografía simétrica y asimétrica; la llave simétrica es utilizada como llave de sesión, es decir, sólo se usa una vez y es generada como un número pseudoaleatorio para cada mensaje; esta llave se añade al mensaje, y para protegerla, se cifra con la llave pública del destinatario. Para incluir una firma digital, se genera dicha firma y se añade al mensaje formando un bloque, éste último se comprime y se cifra con la llave de sesión. Finalmente la llave de sesión se cifra con llave pública y se adhiere al bloque ya cifrado, lo que proporciona el servicio de autenticación.

La conversión Radix-64 se requiere debido a que la representación de los mensajes cifrados, certificados, firmas, y llaves conforman un flujo de octetos arbitrarios. Como algunos sistemas (agentes de correo electrónico o sistemas operativos) sólo permiten el uso de bloques de 7 bits, se necesita una codificación de octetos binarios a caracteres imprimibles para poder transmitir el flujo de octetos binarios a través de canales que no aseguran el flujo de información íntegra. A esta conversión de un flujo de un octeto binario de 8-bit a un flujo de caracteres ASCII imprimibles se le llama codificación Radix-64 o ASCII Armor. El uso de Radix 64 expande un mensaje alrededor del 33%.

PGP comprime el mensaje después de aplicar la firma pero antes de cifrar, lo que trae como beneficio el ahorro de espacio para transmisión de correo electrónico y almacenamiento de archivos. De hecho, debido al algoritmo de compresión de PGP, se producen distintos rendimientos en velocidad de ejecución, produciendo a su vez distintas formas de compresión. Sin embargo, los diferentes resultados son interoperables porque cualquier versión del algoritmo puede descomprimir correctamente la salida de cualquier otra versión.

[35] International Traffic in Arms Regulations. Organismo que vigila el tráfico de artículos de defensa a través de los Estados Unidos; las herramientas criptográficas son consideradas como artículos de defensa (armas) por el gobierno de ese país.

PGP puede utilizarse de maneras diversas, por ejemplo, aplicando el hash y firma después de comprimir podría restringir todas las implementaciones de PGP; mientras que, cifrar el mensaje después de la compresión fortalece la seguridad criptográfica.

Por su parte, el correo electrónico se restringe siempre a una longitud máxima del mensaje; por ejemplo, algunas facilidades accesibles por medio de Internet imponen una longitud máxima de 50,000 octetos.

Para adecuar esta restricción, PGP subdivide automáticamente un mensaje largo en segmentos pequeños separados. La segmentación se hace después de todos los demás procesos, incluyendo la conversión Radix-64.

Para la administración de llaves, PGP utiliza distintas variantes, como el tiempo; además, existen algunos identificadores llamados genéricamente S2K (String-to-Key) que se almacenan en el llavero y sirven para convertir una frase en una llave simétrica, que a su vez será usada para cifrar la llave privada que se almacena en el llavero y para usarla como llave de sesión para el mensaje.

Los identificadores pueden ser de tres tipos. El primero es “Simple S2K”, el cual toma directamente la palabra clave y genera un hash para producir la llave de sesión. El segundo es “Salted S2K”, que incluye una “Salt“[36] y que pasa por la función hash. El tercer tipo es conocido como “Iterated and Salted S2K”, que es una iteración del hash resultante de la “Salt” y la frase. Para distinguir el algoritmo con que se generó un mensaje, PGP utiliza identificadores cuya la preferencia se establece de acuerdo al algoritmo de que se trate; sin embargo, el usuario puede seleccionar el orden de los algoritmos.

PGP utiliza diferentes algoritmos, como RSA, ElGamal y DSA, cuyas llaves de menor tamaño son de 768 bits; sin embargo, en PGP versión 7, la llave más pequeña permitida es de 1024, y para RSA, se permite una llave de hasta 4096 bits.

A pesar de sus ventajas, PGP tiene algunos puntos sensibles, principalmente en la palabra clave y en la llave privada; aunque también la llave pública puede ser un punto vulnerable, ya que es susceptible a ataque por “hombre en medio”, provocando que el llavero que guarda las llaves públicas sea susceptible a ataques.

Por otro lado, el borrado de archivos también puede acarrear problemas, ya que cuando se cifra un mensaje, el texto en claro “se borra” para el usuario, aunque físicamente la información continúa ahí.

Debido a los problemas legales con los que nació PGP, existen varias distribuciones, por lo que el grupo de trabajo de IETF conocido como “OpenPGP” se ha encargado de definir formatos estándar para el cifrado de mensajes, firmas y certificados para el intercambio de llaves públicas, lo que permite implementar PGP sin tener que pagar por la licencia.

[36] Término inglés que puede ser traducido como “sal”, que hace referencia a alguna operación que sirve para darle “consistencia” a la función.

Kerberos

Es un sistema de autenticación desarrollado en el *Massachusetts Institute of Technology (MIT)*, cuyo nombre proviene del perro mitológico de tres cabezas llamado "cancerbero" que cuidaba la salida del infierno. Kerberos sirve para autenticar usuarios y servicios, y también para demostrar la posesión de un secreto (o llave privada) sin necesidad de revelar el secreto mismo.

Kerberos realiza la autenticación de manera similar a como se realiza en la vida real, es decir, a través de un documento expedido por una autoridad certificadora; de esta manera, Kerberos emite boletos (tickets) para los usuarios y para los servicios. Cuando un usuario de red intenta usar algún servicio, debe presentar un boleto que es utilizado por el *Servicio de Autenticación (AS)* de Kerberos (como si fuera la licencia de conducir de un automovilista que el oficial de tránsito examina).

Luego, el servicio examina el ticket y verifica la identidad del usuario. Así, el ticket debe demostrar que el portador conoce algo que sólo el usuario auténtico conoce (un secreto o contraseña); por ello, el ticket debe estar asegurado contra robo y evitar que algún atacante pueda usarlo más tarde. Sin embargo, Kerberos requiere que el usuario y el servicio hayan acordado previamente sus llaves con el Servicio de Autenticación (AS).

Por eso, la *llave del usuario* se deriva de una contraseña que el usuario elige, y la *llave del servicio* se selecciona aleatoriamente, lo que evita que el usuario tenga que teclear una contraseña. Además, en cada mensaje intercambiado, se agrega una "lectura de tiempo" ("timestamp") para que los mensajes intercambiados anteriormente no sean reutilizados por algún atacante.

Kerberos incluye también un agente llamado *TGS ("Ticket Granting Server" o Servidor de Tickets)* distinto del AS[37], cuya función es emitir otro ticket llamado *TGT ("Ticket Granting Ticket")* que sirve sólo por un periodo muy corto (típicamente 8 horas); después de ese tiempo, el TGT no es usable ni por el usuario ni algún atacante.

Este esquema es útil cuando los requerimientos son pequeños, sin embargo, conforme la red crece, el número de requerimientos también crece y el proceso de autenticación se convierte en un cuello de botella.

Una solución es dividir la red en Reinos o Dominios; así, cada reino tiene su propio AS y su propio TGS. Para permitir a un usuario de un reino utilizar servicios de otro reino, es necesario que el reino del usuario registre un "TGS Remoto" (RTGS). En algunos casos, donde hay muchos reinos, este esquema es ineficiente, por eso, en Kerberos Versión 5 se utilizan Jerarquías de Reinos, de tal modo que para contactar un servicio en otro reino, puede ser necesario contactar el RTGS en uno o más reinos intermedios, por lo que los nombres de cada reino se registra en el ticket.

[37] Tanto el TGS como el AS son conocidos como *Key Distribution Center* (*KDC*) o *Centro de Distribución de Llaves*.

Secure SHell (SSH)
SSH es un conjunto de herramientas que sirve para realizar autenticación, transferencia de archivos y ejecución de comandos en un equipo remoto en red de manera segura; por ello, SSH puede reemplazar a las herramientas comunes e inseguras como *telnet, ftp, rlogin, rcp* y *rdist,* convirtiéndolo en una herramienta muy potente, fácil de instalar y muy cómoda. Existen diferentes versiones libres de Secure Shell, basadas en la versión 1.2, y aunque existen diferencias de funcionamiento entre ellas, todas implementan un canal de comunicación cifrado y mecanismos de validación de usuarios.

Cuando se inicia la comunicación, se establece el canal en el que cada servidor tiene una llave RSA de 1024 bits; el servidor transfiere sus llaves públicas al cliente, quien las verifica en una base de datos; si la llave es correcta, el cliente genera un número aleatorio de 256 bits (que sirve como llave de sesión) y lo envía al servidor; a partir de este momento todo diálogo se hace cifrando la comunicación con esa llave de sesión. Después de la conformación del canal, SSH valida al usuario usando uno de varios mecanismos, de los cuales, algunos se utilizan solo para guardar compatibilidad con rlogin y rsh.

Existen algunas implementaciones de SSH bajo Unix que aceptan la validación por RSA y también a través de contraseñas de Unix. Así, una vez que el usuario fue validado, se realiza una negociación para seleccionar detalles del tipo de conexión, y finalmente, se ejecuta un shell o cualquier comando que se desee. Existen diferentes distribuciones, como la versión 1.2 que es de carácter comercial, sin embargo, existe una versión no comercial, que se puede utilizar con la única restricción de no lucrar con ella. De hecho, SSH es considerado como estándar para los intérpretes de comandos seguros.

Tomando en cuenta los programas criptográficos mencionados anteriormente, no existen criterios que ayuden a determinar al “mejor”. Cuando se intenta elegir algún software de seguridad se debe tener en cuenta el objetivo a lograr, es decir, los servicios de seguridad (fig 2.11), así como los intereses y formas de trabajo de la organización.

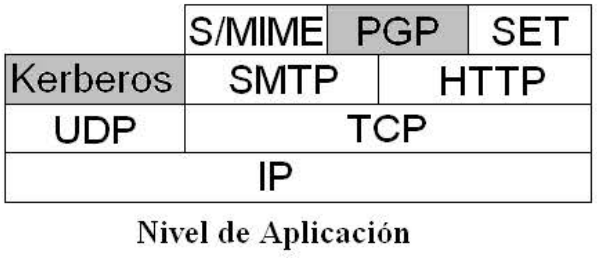


Fig 2.11. Aplicaciones Criptográficas

2.4.3 Seguridad en Web
El Web es una aplicación cliente/servidor ejecutándose sobre Internet e Intranet TCP/IP; en este esquema, Internet funciona de manera bidireccional, lo que lo hace vulnerable a ataques. Por ejemplo, un servidor Web puede utilizarse como plataforma de ataque a los sistemas de alguna organización, donde el atacante es capaz de tener acceso a los datos y sistemas conectados al servidor localmente.

Además de los problemas que enfrenta el Web, existen otras situaciones que ponen de riesgo, como la falta de seguridad en los sistemas operativos, los problemas inherentes a los firewalls, y principalmente, los usuarios inexpertos (en seguridad).

Una forma de proporcionar seguridad en el Web es usar IPSec, ya que es transparente a los usuarios y a las aplicaciones, e incluye la capacidad de filtrado. Otra solución es implementar seguridad justo arriba de TCP, tal como lo hace el protocolo SSL y el estándar derivado de SSL para Internet llamado TLS, descritos en seguida.

Secure Socket Layer (SSL)

SSL es software criptográfico desarrollado por Netscape, que emplea las funciones de autenticación mutua, cifrado e integridad de datos para transacciones seguras. La versión 3 del protocolo fue diseñada bajo revisión pública, luego, cuando se logró consenso para proponerlo como estándar de Internet, se formó el grupo de trabajo para TLS dentro del IETF con el fin de desarrollar la norma. En la actualidad, el trabajo sobre TLS pretende producir una versión inicial como Estándar de Internet, definida en el RFC 2246.

SSL usa criptografía de llave pública para autenticación mutua y cifrado de la llave de sesión entre el navegador y el servidor, además usa cifrado de llave simétrica para cifrar la sesión mediante una llave diferente para cada conexión cliente/servidor. Existen dos formas de implementación; en la primera, SSL (o TLS) puede implementarse como parte de la plataforma del conjunto de protocolos para hacerlo transparente a las aplicaciones; la segunda, es incrustar los servicios de seguridad específicos para aplicación dentro de la aplicación misma; la ventaja de este enfoque es que el servicio puede ajustarse a las necesidades de la aplicación (fig 2.12).

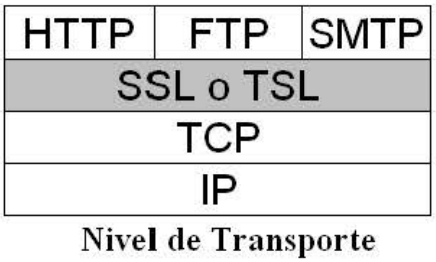


Fig 2.12. Nivel de Implementación de SSL

SSL es un conjunto de tres protocolos de capa superior: Al primero se le conoce como *"Handshake Protocol"*, y se encarga de definir la llave secreta compartida usada para cifrado convencional, dando confidencialidad e integridad a los mensajes; además permite al servidor y al cliente autenticarse entre sí, y negociar algoritmos para cifrado, MAC y llaves criptográficas. SSL se usa antes de la transmisión de cualquier dato de aplicación y consiste en una serie de mensajes intercambiados entre el cliente y el servidor.

El segundo protocolo se conoce como *"Change Cipher Spec Protocol"* y consiste en un mensaje formado por un byte único de valor 1, cuyo propósito es provocar el estado de espera, que a su vez define la suite de cifrado usado para la conexión.

El tercer protocolo es *"Alert Protocol"* y se usa para transportar alertas SSL relacionadas a las entidades. Cada mensaje consiste de dos bytes, donde el primero toma el valor warning (1) o fatal (2) para comunicar la severidad del mensaje; el segundo byte contiene un código que indica la alerta específica. Estos protocolos se usan en el manejo de intercambios SSL, pero también pueden incrustarse en paquetes específicos, como los navegadores Netscape o Microsft Internet Explorer.

2.4.4 Firewalls[38]

En la actualidad, el acceso a Internet implica muchas ventajas pero también representa riesgos para la organización, ya que, así como se puede interactuar dentro de la red hacia fuera, puede suceder en sentido contrario, permitiendo a algún atacante interactuar con los recursos de cómputo de alguna organización.

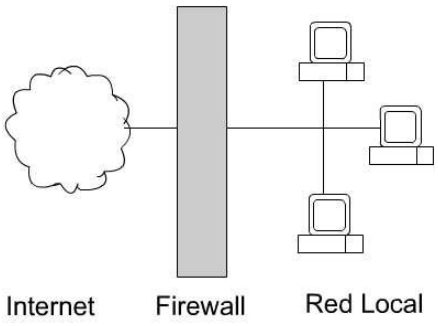


Fig 2.13. Implementación de Firewall

Por ello, en la mayoría de las organizaciones se opta por equipar al servidor de programas antivirus y de detección de intrusos, que aunque ofrecen cierta seguridad, son insuficientes para proteger el perímetro. Una opción más viable para implementar seguridad es el uso de un firewall, el cual se inserta entre la LAN e Internet para establecer un enlace controlado y levantar una pared de seguridad perimetral (fig. 2.13), protegiendo la red contra accesos no autorizados y brindando un único punto de acceso donde se implementa seguridad y auditoria en la red de la organización.

El firewall examina los paquetes IP que viajan entre el servidor y el cliente, definiendo un punto de entrada y salida únicos, simplificando la administración de la seguridad y evitando que servicios vulnerables entren o salgan de la red; también puede servir para realizar funciones de Internet no relacionadas con seguridad, como la traducción de direcciones de red, el mapeo de direcciones locales a direcciones de Internet o servir como plataforma para IPSec.

Existen cuatro técnicas generales para filtrar el tráfico que pasa por el firewall. La primera es conocida como *"Control de Servicio"*, que determina precisamente los servicios de Internet que se pueden accesar hacia adentro o hacia fuera, y filtra el tráfico en base a la dirección IP y en el número de puerto TCP.

Otra técnica es el *"Control de Dirección"*, que determina la dirección en la que pueden iniciarse los servicios, permitiéndoles pasar a través del firewall. Por su parte, el *"Control de Usuarios"* controla el acceso a los servicios de acuerdo al usuario que intenta el acceso. Por último, el *"Control de Conducta"*, ayuda a verificar la forma en que se utilizan los servicios; por ejemplo, el firewall puede filtrar correo electrónico para eliminar spam.

A pesar de la seguridad que ofrecen, los firewalls tienen algunas limitaciones, por ejemplo, no pueden proteger contra amenazas internas (como empleados descontentos), ni proteger contra la transferencia de archivos infectados por virus; además, representan un potencial cuello de botella porque todas las conexiones tienen que pasar y ser examinadas por él.

Los firewalls son diferentes entre sí por su forma de operación y están enfocados a distintos usos, por ejemplo:

[38] El término Firewall es traducido al castellano como "cortafuegos".

Firewall de Filtrado de Paquetes.
En este esquema se configura el ruteador para filtrar paquetes desde y hacia la red (fig 2.14), basándose en reglas de filtrado incluidas en una lista de coincidencias en los campos de encabezados IP o TCP; así, cuando ocurre una coincidencia, el paquete se reenvía o se descarta; si no existen coincidencias, se toma una acción por omisión:

***Default* = *discard*: Lo que no está expresamente permitido, está prohibido**
***Default* = *forward*: Lo que no está expresamente prohibido, está permitido**

El ruteador puede filtrar paquetes IP basado en algunos campos, como la IP de origen o destino, o el puerto origen o destino TCP/UDP, de manera que se pueden bloquear conexiones TCP o UDP hacia o desde puertos específicos, e implementar políticas que permitan que ciertas conexiones puedan realizarse a ciertos hosts.

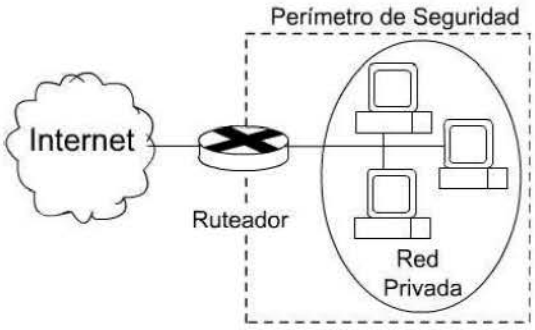


Fig 2.14. Firewall de Filtrado de Paquetes.

Este tipo de firewall es el más común y fácil de emplear, ya que es rápido y transparente para los usuarios; sin embargo, presenta algunas desventajas evidentes; por ejemplo, las reglas de filtrado son difíciles de examinar, llegando a ser inmanejables; además, tiene una capacidad de registro de eventos muy pequeña, lo que dificulta el seguimiento. Pero la desventaja mayor es que los ataques principales se realizan sobre este tipo de firewalls.

Para reducir sus vulnerabilidades, los firewalls utilizan aplicaciones de software para reenviar y filtrar conexiones para servicios como telnet y ftp; estas aplicaciones se conocen como Servicios Apoderados o "proxy", mientras que el host que ejecuta el servicio proxy se conoce como "Gateway de Aplicación".

Gateway de Nivel Aplicación
En este esquema, el firewall regulado el tráfico de aplicación, de manera que el usuario contacta al gateway mediante una aplicación TCP/IP (como telnet o ftp); luego, el gateway pregunta al usuario el nombre del host remoto accesado.

Cuando el usuario responde con un ID válido, el gateway contacta la aplicación en el host remoto y pasa segmentos TCP con datos de la aplicación entre los dos puntos finales, resultando fácil de registrar y auditar el tráfico entrante a nivel aplicación (fig 2.15).

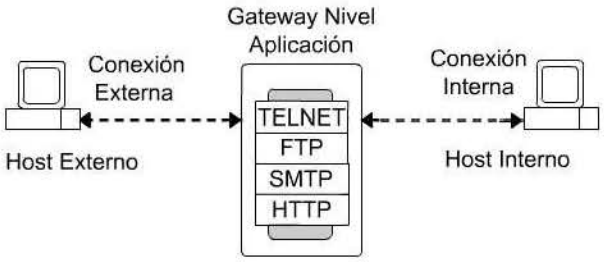


Fig 2.15. Gateway de Nivel de Aplicación.

Una desventaja de este esquema es el procesamiento adicional en cada conexión, ya que existen dos conexiones empalmadas entre usuarios finales, por lo que el gateway debe examinar y reenviar todo el tráfico en ambas direcciones.

Gateway de Nivel Circuito

En este esquema se definen dos conexiones: una entre el gateway mismo y un usuario TCP interno, y otra entre el gateway y un usuario TCP externo, de manera que cuando las dos conexiones se establecen, el gateway pasa segmentos TCP de una conexión a otra sin examinar los contenidos (fig 2.16).

En este caso, la función de seguridad consiste en determinar las conexiones permitidas; por otro lado, el gateway puede configurarse para soportar el *servicio proxy* en conexiones entrantes y funciones a *nivel circuito* para conexiones salientes.

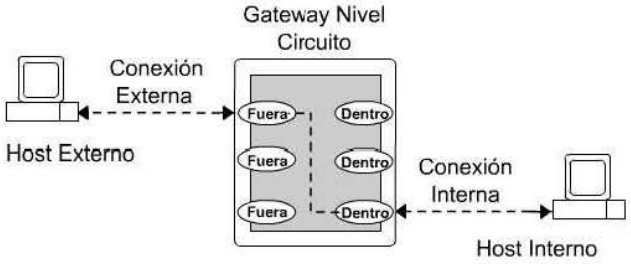


Fig 2.16. Gateway de Nivel de Circuito.

Host Bastión

Un firewall de este tipo se conoce también como “Anfitrión de Doble Domicilio” y consta de un host con dos interfaces de red y una IP del host sin capacidad de reenvío, es decir, el anfitrión no puede prolongar el ruteo de paquetes entre las dos redes conectadas. Las computadoras externas se comunican con una interfaz y las computadoras internas se comunican con la otra tarjeta, de manera que el host bastión sirve como plataforma para un gateway de nivel aplicación o nivel circuito.

El host bastión puede requerir autenticación adicional antes de permitir a un usuario acceso a los servicios del proxy; además, cada servicio proxy puede requerir su propia autenticación antes de otorgar el acceso al usuario. De esta manera, cada proxy se configura para permitir acceso sólo a hosts específicos, por lo que los comandos pueden aplicarse sólo a un subconjunto de sistemas de la red protegida. Por otro lado, cada proxy mantiene información detallada de auditoría registrando el tráfico, la conexión, y duración de cada conexión; este registro es esencial para descubrir y terminar ataques.

Como un proxy no realiza accesos a disco, se dificulta al atacante la instalación de caballos de troya, sniffers o algún otro código malicioso; además, cada proxy se ejecuta como usuario no privilegiado en un directorio privado y seguro.

En un host bastión, el proxy que soporta el servicio podría restringir el acceso basándose en el usuario, la máquina, o la red, además de decidir quién tiene acceso al servicio. Es importante considerar que si el servicio está comprometido, el firewall ya no protegerá el resto de la red, por lo que se debe contar con un plan para lidiar con fallas y probar el firewall de manera exhaustiva.

Aunque se trata de un firewall sencillo, es muy seguro, ya que el ruteador puede evitar accesos directos de Internet al firewall y obligar que todos los accesos sean a través de éste. Además, se logra la negación de los servicios, a menos que estén específicamente permitidos. Además, se logra un alto grado de privacidad ya que los nombres y direcciones IP de los sistemas del sitio se ocultan a los sistemas de Internet debido a que el firewall no pasa información al DNS.

De manera general, para instalar y configurar un firewall se necesitan conocer previamente las políticas de seguridad de la organización, así como la forma en que se comunica el servicio con sus clientes, con el fin de entender las posibles ubicaciones del servicio con respecto a la topología del firewall y los riesgos derivados de la ubicación.

En este capítulo se resumen a grandes rasgos los temas más importantes revisados durante el Diplomado de Seguridad Informática de la UNAM, tales como los fundamentos de la criptografía y sus aplicaciones en la seguridad actual; también se revisaron los procedimientos para emitir políticas de seguridad dentro de una organización y los conceptos básicos de la seguridad en redes. Todos estos antecedentes brindan un panorama general de la seguridad y ayudan a comprender los capítulos posteriores de este trabajo.

3

CÓDIGO MALICIOSO Y VIRUS INFORMÁTICOS

En el capítulo anterior se realizó una síntesis de la seguridad informática, lo que proporciona amplio un panorama sobre los tópicos que involucra este tema y sus distintas aplicaciones. En el presente capítulo trata sobre Virus Informáticos y Código Malicioso, el cual ha evolucionado a lo largo del tiempo junto con las Tecnologías de la Información. Los ataques a través de código malicioso son cada vez más frecuentes, letales y costosos, por lo que es importante estudiarlos detalladamente.

3.1 Código Malicioso.

El código malicioso (ó maleware[39]) se refiere a programas diseñados por gente sin escrúpulos, con la intención específica de dañar o corromper un sistema de cómputo; estos programas son clasificados de acuerdo a su modo de ejecución, su forma de propagación o sus efectos. No existe una clasificación formal, ya que muchos autores consideran cierto tipo de software dentro de la clasificación, dejando fuera otros que pudieran ser considerados por otros autores.

Los programas maliciosos se han convertido en una verdadera amenaza, tanto para los activos físicos de una organización como para sus finanzas, debido a que puede llegar prácticamente por cualquier medio: dispositivos removibles, un archivo compartido en la red, correo electrónico, Internet y más. Lo peor, es que llegan, casi siempre, de manera inadvertida para el usuario y también para el encargado de los sistemas.

Un ataque con código malicioso representa pérdida en la productividad de la organización, una gran inversión de recursos humanos y económicos para eliminarlo, y sobre todo, pérdida de reputación y prestigio. Este capítulo pretende estudiar a detalle la mayor parte de los problemas considerados como código malicioso.

3.2 Virus.

Los virus informáticos representan el tipo de código malicioso más antiguo que se conoce; para comprenderlos mejor, se describirá la forma en que actúa un virus biológico y se hará una analogía con un virus informático, ya que ambos actúan de manera muy similar, es decir, necesitan un agente de infección, un medio de transmisión y un huésped que alojará la infección hasta que ésta se dispare bajo ciertas condiciones.

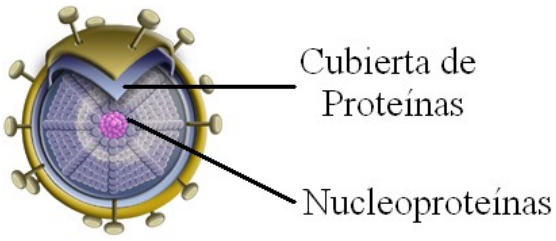


Fig 3.1. Virión y sus partes

Un virus biológico es una gran molécula compleja llamada “virión”, formada por un núcleo de ácido nucleico (“nucleoproteína”) rodeado de una cubierta de proteína. El ácido nucleico de un virus puede ser ADN[40] si se trata de un virus animal, o ARN[41] si es virus vegetal. Un virus no está formado por células pero puede realizar funciones biológicas (como la reproducción), y llegar a cristalizarse (al igual que una sustancia química).

[39] Palabra que se tomó de la frase en inglés “Malicious Software”
[40] ADN. Ácido Desoxirribonucleico
[41] ARN. Ácido Ribonucléico

Por lo tanto, los virus no son seres totalmente inanimados, pero tampoco pueden considerarse como seres vivos; pueden ubicarse entre las grandes células inanimadas (como las proteínas) y los organismos vivos más sencillos (como la ameba).

Un virus contiene toda la información necesaria para su ciclo de reproducción, y necesita la materia y la energía de otras células vivas para reproducirse. Fuera de la célula huésped, el virión es tan inerte como cualquier molécula de proteína o ácido nucleico, pero una vez dentro, es capaz de manifestar sus propiedades biológicas. No crece en la célula huésped, sino que se divide formando células víricas idénticas.

Un virus puede actuar de dos formas distintas: la primera, reproduciéndose en el interior de la célula infectada (huésped) utilizando todo su material y energía; la segunda, uniéndose al material genético de la célula en la que se aloja, produciendo cambios genéticos en ella. Por eso, los virus son considerados agentes infecciosos productores de enfermedades o agentes que alteran el material genético hereditario de la célula huésped.

3.2.1 Historia de los Virus Informáticos.

La idea de generar un programa capaz de reproducirse se le atribuye a John Von Neumann por su artículo *"Theory and Organization of Complicated Automata"* escrito en 1949. En él, Von Neumann habla sobre la creación de “vidas artificiales electrónicamente” llamadas “autómatas”, que podían reproducirse con facilidad. Con estos conceptos, se sentaron las bases técnicas de los virus mediante el concepto de "programa almacenado", que hacía que programas y datos se almacenaran conjuntamente en la memoria, lo que permitía que el código fuera alterado.

Existen dos teorías sobre el origen de los virus informáticos; la primera de ellas plantea que cuando empezaban a desarrollarse las primeras computadoras, se tuvo la necesidad de llevar a éstas a un estado inicial conocido, eliminando rastros de otros programas previamente cargados. Una solución a este problema consistía en implementar una instrucción que se copiaba a la siguiente posición de memoria y saltaba a ella para seguir ejecutándose. De esta forma todo el mapa de memoria se llenaba con un único valor conocido, es decir, el código correspondiente a la instrucción, con lo que se producía código capaz de reproducirse.

La segunda teoría (y la más aceptada) indica que durante los años 60, cobró gran popularidad el juego "Core Wars", diseñado (entre otros investigadores) por Ken Thomson en los Laboratorios Bell de AT&T. El juego consistía en que dos jugadores iniciaban simultáneamente un programa llamado “organismo”, y a partir de una señal, el “organismo” se reproducía en memoria hasta que ésta se agotaba; ganaba aquel que fuera capaz de "conquistar" más espacio en memoria y era legal "matar" a las copias del adversario y "robarle" esa memoria.

Durante el juego, los programas debían “sobrevivir” usando técnicas de ataque, ocultamiento y reproducción, similares a las de los virus informáticos actuales; al término del juego, se borraban de memoria los rastros del programa, ya que estas actividades eran severamente sancionadas por representar un gran riesgo. “Core Wars” fue muy conocido entre gente relacionada con el cómputo, pero no se dio a conocer hasta 1983.

En ese año, Ken Thomson recibió el premio *“A.M. Turing de A.C.M.”.* En su discurso, basado en el juego "Core Wars" anima a la experimentación con esas "criaturas lógicas", y presentó varios experimentos donde demostraba su factibilidad; probó las limitaciones para defenderse de ellos y la imposibilidad de diseñar un sistema de detección universal.

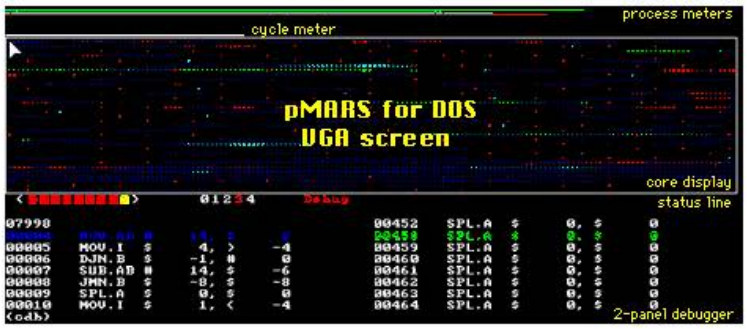


Fig 3.2. Interfaz del Juego “Core Wars”

Luego, la revista *Scientific American* dio difusión a “Core Wars”, provocando que sus lectores experimentaran con ellas, derivando en la aparición de los primeros virus. Por otro lado, Fred Cohen, autor del primer virus informático conocido, experimentó en una computadora VAXII / 750 con un programa que *"pudiera modificar otros e incluir una copia (evolucionada) de sí mismo".*

Definió por primera vez a los virus informáticos mientras dictaba la conferencia *"Computer Viruses Theory and Experiments"*, en la que mencionó:

"Definimos a un virus informático como un programa capaz de infectar otros programas, modificándolos para incluir una pequeña copia de él mismo. Un virus puede propagarse a través de sistemas de cómputo o redes de computadoras usando la autorización de cada usuario para infectar sus programas. Cada programa que ha sido infectado puede actuar como virus, por eso, la infección crece”.

Se considera que la primera generación de los virus surge en 1985, e incluye virus de archivo, de sector de arranque y de partición (estudiados más adelante en este capítulo). El primer virus fue desarrollado en Pakistán por Basit y Amjads, quienes inicialmente habían creado un programa no dañino llamado “Ashar”, que evolucionó en el virus *“Brain”*.

“Brain” sobrescribía el sector de arranque de los antiguos disquetes de 5.25” y desplazaba el sector de arranque original a otra posición. Aunque el virus apenas provocaba daños, llamaba la atención su capacidad de ocultamiento, ya que fue el primero en utilizar la técnica *stealth* (estudiada mas adelante), con lo que el disquete infectado mostraba una apariencia normal, por eso, el virus no fue descubierto sino hasta 1987. En la Universidad de Delaware se detectaron las primeras infecciones masivas; los encargados de la red notaron que tenían un virus porque se desplegaba el mensaje "© Brain" como etiqueta de los disquetes. En 1986 surge el virus “VIRDEM”, que podía copiarse a sí mismo y anexar una copia a otros archivos con extensión *.com*.

Durante este periodo, los virus tuvieron una propagación lenta y limitada, porque el único medio de transmisión era de disquete a disquete, ya que la mayoría de las computadoras no contaban con disco duro. La segunda generación de los virus aparece en 1995 con los virus de macro; en 1999 apareció la tercera generación con todos los virus transmitidos por Internet. La cuarta generación inicia con los virus ”*Melissa”* y *“Explore.zip”* que utilizaban nuevas técnicas de propagación y ocultamiento mas avanzadas.

3.3 Fundamentos de los Virus.

Un virus es una pequeña pieza de código ejecutable que se replica y adjunta a otro archivo; tiene como efecto provocar un mal funcionamiento del equipo infectado, dañar o modificar datos, mostrar mensajes o corromper el sistema. El objetivo principal de un virus es infectar un sistema de cómputo y esparcirse rápidamente hacia otros equipos.

La palabra "virus" se tomó del acrónimo de la frase en inglés *"Vital Information Resources Under Siege"*, que puede traducirse como '*Recursos Informáticos Vitales Bajo Amenaza';* este acrónimo y la similitud con los virus biológicos, dieron nombre a los virus informáticos.

Los virus son escritos generalmente para una aplicación, ambiente o sistema operativo en específico, y rara vez pueden infectar todo tipo de plataformas. Los sistemas operativos más vulnerables a un ataque de virus son las familias de Windows, ya que su uso común y las numerosas vulnerabilidades que presentan son un objetivo muy fácil de explotar. Además, como los desarrolladores de virus han mejorado sus habilidades, los virus incorporan técnicas para reproducirse cada vez más rápido.

Los virus son creados por programadores experimentados, que argumentan que, con sus creaciones, sólo tratan de hacer notar la falta de seguridad informática; a este tipo de individuos se les conoce popularmente como "hackers" quienes, agrupados en distintos grupos en varios países, han generado cierta competencia por crear virus más nocivos.

Los virus también son escritos por los llamados "wanabees"[42], adolescentes solitarios, con problemas de integración familiar, con mínimos conocimientos de computación y que actúan de manera individual; toman un virus que ya había sido escrito y lanzado en ataques previos, lo modifican y lo vuelven a lanzar, dando origen a nuevas variantes de virus. Actualmente se conocen más de 250,000 virus, y semanalmente se descubren alrededor de 300 virus nuevos alrededor del mundo[43]. Existen similitudes entre los virus informáticos y los virus biológicos, descritas en el siguiente cuadro:

Virus Biológicos	Virus Computacionales
Ataca células específicas de un cuerpo.	**Ataca programas específicos (archivos .exe, .com, entre muchos otros).**
Modifica información genética de una célula.	**Manipula un programa para ejecutar una tarea.**
Nuevos virus crecen por sí mismos en la célula infectada.	**El programa infectado produce virus.**
Una célula no es infectada más de una vez.	**Un programa es infectado una sola vez por la mayoría de los virus.**
Un organismo infectado puede no mostrar síntomas en largo tiempo.	**Un programa infectado puede funcionar sin errores durante largo tiempo.**
No todas las células con las que el virus entra en contacto son infectadas.	**Los programas pueden ser inmunes contra ciertos virus.**
Los virus pueden mutar, por eso no pueden ser descritos completamente.	**Los virus pueden modificarse a sí mismos, lo que les puede ayudar a no ser detectados.**

[42] Palabra coloquial en inglés que significa "querer ser".
[43] Fuente: McAfee. www.nai.com

Estas similitudes han motivado que, algunos investigadores de cómputo se apoyen en colegas del área de infectología médica, aprovechando sus conocimientos sobre virus biológicos y aplicándolos en investigaciones sobre virus informáticos, logrando excelentes resultados. Así, se han obtenido importantes datos sobre los virus informáticos, por ejemplo, que la velocidad de infección de una red es directamente proporcional al número de equipos infectados y al número de máquinas limpias, lo cual se puede expresar como**:**

$$dx / dt = kx\,(N - x)$$

donde: x = *cantidad de equipos infectados,* t = *tiempo*

N = *Número total de equipos,* k = *Constante de proporcionalidad*

Integrando, se tiene: $$\int_{x_0}^{x} \frac{dx}{x(N-x)} = k\int_{t_0}^{t} dt \quad \Longrightarrow \quad \frac{x}{N-x} = \frac{x_0}{N-x_0} e^{Nk(t-t_0)}$$

Así, se puede determinar que cuando el número de equipos infectados es pequeño en relación al número total de equipos, los equipos infectados crecen de manera exponencial; mientras que, al aumentar el número de equipos infectados, la velocidad de propagación del virus disminuye debido a un fenómeno de saturación. Graficando la ecuación se obtiene (Fig 3.3):

En la gráfica se observa el comportamiento de un virus con respecto al tiempo, lo que permite concluir que, mientras el virus se encuentre en pocos equipos (fig. 3.3, línea punteada) su velocidad de reproducción es menor, por lo tanto, es más fácil erradicarlo. Pero si no se tiene un tiempo de respuesta adecuado, el virus se reproducirá cada vez de manera más rápida, llegando a infectar un número de equipos mucho mayor, dificultando su erradicación. La gráfica llega a ser constante debido a que en ese momento ya se han infectado la totalidad de equipos en la red.

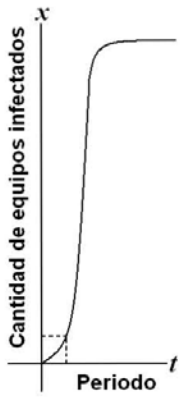


Fig 3.3. Reproducción de virus con respecto al tiempo

3.3.1 Las Partes de los virus

Los virus cuentan con cuatro partes que los distinguen de los demás tipos de *maleware*; cada componentes, realiza funciones específicas que al combinarse con las demás, forman una pieza de código que migra de un sistema a otro e inicia su efecto dañino.

Reproducción

Es un mecanismo, también conocido como *Réplica,* que permite transmitir el virus a un nuevo archivo; es el único componente característico de un virus, ya que ningún otro tipo de código malicioso es capaz de reproducirse.

Ocultamiento

También conocido como *Stealth* por su nombre en inglés; es una técnica que permite a un virus pasar desapercibido el mayor tiempo posible para evitar que sea detectado por los programas antivirus y así, iniciar una infección masiva.

Si un virus no actuara de manera oculta, sería identificado y eliminado de inmediato; por ello es que las técnicas de ocultamiento son indispensables para alargar el ciclo de vida de un virus.

Cuando un virus infecta un archivo suele dejar signos evidentes: variación en el tamaño, modificación de la fecha u hora de creación, sectores marcados como defectuosos y más. El virus hará que cada una de estas posibles pistas no puedan ser visualizadas, para ello vigilará las peticiones del sistema operativo, interceptándolas y ofreciendo información falsa o irreal a través de diferentes técnicas de ocultamiento, entre las que se encuentran:

Cifrado. Esta técnica permite al virus actuar de forma diferente en cada infección, esto es, que utilizará una cadena concreta (llamada firma de virus) para realizar una infección, y en la siguiente infección usará una cadena distinta. Además, el virus cifra sus cadenas para que al programa antivirus le sea difícil encontrarlo, pero, como los virus emplean siempre el mismo algoritmo de cifrado, es posible su detección.

Tunneling. Esta técnica se utiliza para tener control sobre todos los servicios ofrecidos por las interrupciones del sistema; este método requiere una programación compleja, ya que tras ejecutarse una instrucción y producirse una interrupción, se coloca una ISR[44] para dicha interrupción; luego, se ejecutan instrucciones comprobando cada vez si se ha llegado al objetivo hasta recorrer la cadena de ISR's colocadas al final.

Todas las operaciones que se realizan sobre cualquiera de los archivos son inspeccionadas por el antivirus mediante la intercepción de las acciones que el sistema operativo lleva a cabo. De la misma manera, el virus intercepta estas peticiones, obteniendo las direcciones de memoria en las que se encuentran, así el antivirus no detectará la presencia del virus.

Debugger. Es un programa que permite descompilar programas ejecutables y mostrar su código en lenguaje original. Los virus usan técnicas llamadas "antidebuggers" para evitar ser desensamblados e impedir su análisis para desarrollar el antivirus correspondiente.

Polimorfismo. También conocida como *mutación*, es una técnica que cambia el código del virus en cada infección (como lo hace el virus del SIDA en los humanos) y además, cifra el algoritmo de infección. Así, el virus crea ejemplares de sí mismo diferentes cada vez, cambiando de "forma" en cada una de ellas. Como una parte del virus toma el control, esa parte queda sin mutar y sin cifrar, por ello, el virus queda vulnerable al programa antivirus. Por su parte, el antivirus usa técnicas heurísticas y de simulación de descifrado (analizadas en el capítulo siguiente) para eliminar al virus.

La forma más utilizada para codificar virus es la operación lógica XOR ya que es reversible; por ejemplo, ***7* XOR *9* = *2*** es reversible, resultando que ***2* XOR *9* = *7***, donde la clave es el número 9, pero utilizando una clave distinta en cada infección se obtiene un cifrado distinto. Otra técnica es sumar un número fijo a cada byte del código del virus.

[44] ISR: Interruption Service Request, petición de interrupción de servicio.

TSR[45]. Los Programas Residentes en Memoria permanecen alojados en ésta durante toda su ejecución; los virus utilizan esta técnica para mantener el control sobre todas las actividades del sistema e infectarlas.

La primera acción del virus al llegar a la memoria es infectar los archivos de arranque del sistema para asegurar que cuando se vuelva a arrancar la computadora, vuelva a ser cargado en memoria, y permanece ahí mientras la computadora esté encendida.

Disparador
Componente conocido también como *Trigger* por su nombre en inglés; consiste en un pequeño código que activa el efecto dañino. Un virus se encuentra generalmente en estado latente, hasta que se cumple cierta condición que lo active e inicie el efecto dañino: un contador, una combinación de teclas, la existencia de un archivo específico, la ejecución de un programa, una fecha u hora específica (llamada también "bomba lógica") o cualquier otra condición; cuando ésta se cumpla comenzará el efecto del virus.

Efecto
Es un el último componente de los virus, conocido también como *Payload; e*s la acción que realiza un virus luego de que la computadora ha sido infectada, por ejemplo: formatear el disco duro, tomar el control del equipo infectado, modificar o borrar datos, detener la ejecución de un programa, o simplemente mostrar un mensaje en pantalla. El efecto de un virus después de una infección puede ser impredecible.

3.3.2 Clasificación de los Virus

La clasificación de los virus se realiza considerando los componentes de la computadora que puede infectar, ya sea software o unidades lógicas de discos (un virus no puede infectar hardware). Para comprender mejor cómo se realiza la infección de un disco duro (o disquete) es importante detallar su funcionamiento lógico.

Cuando se inicia una computadora, la primera rutina que ejecuta es la lectura del BIOS[46]; luego se lee y se ejecuta el contenido del primer sector físico del primer disco duro (o disquete) del sistema. Ese primer sector es el *MBR*[47]*,* un pequeño programa escrito en lenguaje ensamblador que el S.O. utiliza para iniciarse y que se ubica en el *Cilindro 0 Cabeza 0 Sector 1* del disco duro. Al final del MBR se encuentra almacenada la tabla de particiones, programa que sirve para determinar la partición de inicio.

El MBR, se encarga de recorrer la tabla de particiones y validar cuál es la partición lista para arrancar el equipo; luego, pasa el sector de arranque de disco a memoria, y le otorgar el control para cargar y ejecutar el S.O.

[45] Terminate and Stay Resident ó TSR por sus siglas en inglés. Programa Residente en Memoria.
[46] Binary Input / Output System ó Sistema Binario de Entrada/Salida.
[47] Conocido también como "Registro de Inicio Principal" o "Bloque de Inicio Principal".

Por su parte, un disco duro esta formado físicamente por una pila de platos conocida como "cilindro"; cada plato tiene dos lados (0 y 1), que son leídos por su respectivo brazo (fig 3.4).

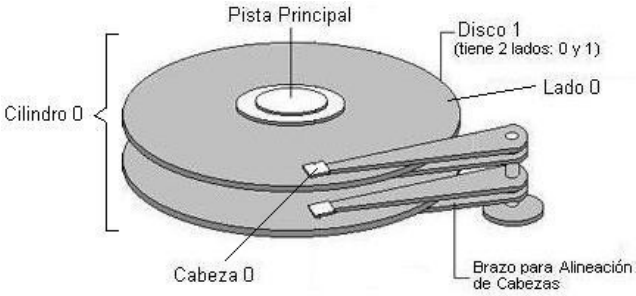


Fig 3.4. Estructura de un Disco Duro

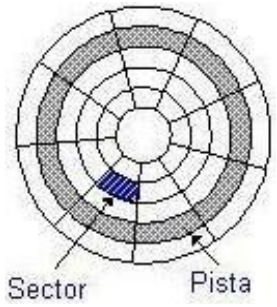


Fig 3.5. Partición de Disco Duro.

Así, cada disco es dividido de manera lógica en *pistas* y *sectores* (fig 3.5) (como si fueran rebanadas de pastel), para ubicar los datos en una lista de archivos (en el caso de Windows se llama FAT[48]) y así, localizar los datos más rápidamente sin necesidad de leer todo el disco completo.

Virus de Partición.

Debido a que la tabla de particiones es leída casi de inmediato al encender la computadora y antes de cargar el S.O., los virus aprovechan esta secuencia para infectar la tabla de partición, lo cual realizan de tres formas distintas: modificando su información, moviéndola a otro sector del disco duro (por ejemplo: *Cilindro 1 Cabeza 2 Sector 16*) (fig 3.6), o borrándola completamente. En todos los casos, el efecto es la pérdida de acceso al disco duro y a los datos alojados.

En un disquete infectado el virus de partición no se manifiesta, ya que puede utilizarse de manera normal sin que el usuario note la presencia de virus. La única forma en que un virus de partición se propaga, es iniciando la computadora con un disquete infectado; así, podrá transferir la información del virus hacia la tabla de partición del disco duro. Un ejemplo bastante conocido de este tipo de virus es el virus "WYX", que surgió hace años y que en la actualidad sigue infectando.

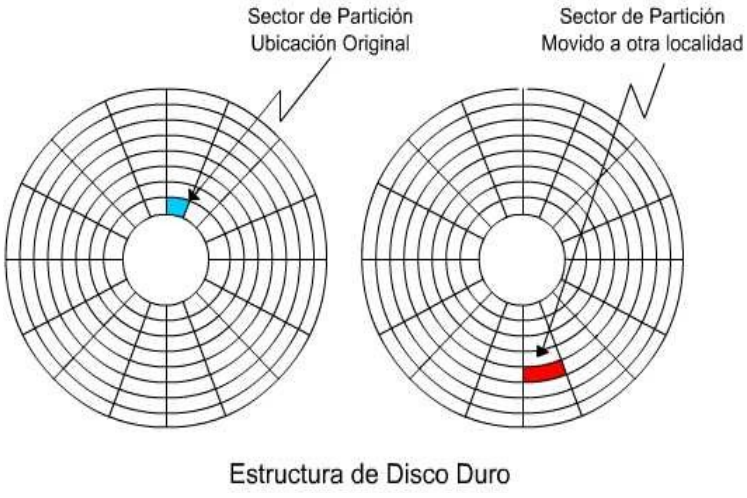


Fig 3.6. Efecto de un Virus de Partición.

[48] File Allocation Table o Tabla de Asignación de Archivos.

Virus de Sector de Arranque.

El sector de arranque de un disco duro contiene información sobre el formato del disco: numero de pistas, sectores, cilindros, sector de inicio, entre otras; además contiene un pequeño programa que verifica si el disco puede iniciar el S.O. Un virus de sector de arranque contiene código que se ejecuta cada vez que la máquina se inicia; entonces, el virus reemplaza ese código con su propio programa residente y continúa con la carga normal del sistema (fig 3.7).

El virus utiliza el sector de arranque y la tabla de particiones para ubicarse, guardando el sector original en otra parte del disco; en ocasiones, el virus marca como defectuoso el sector donde guarda el sector de arranque original.

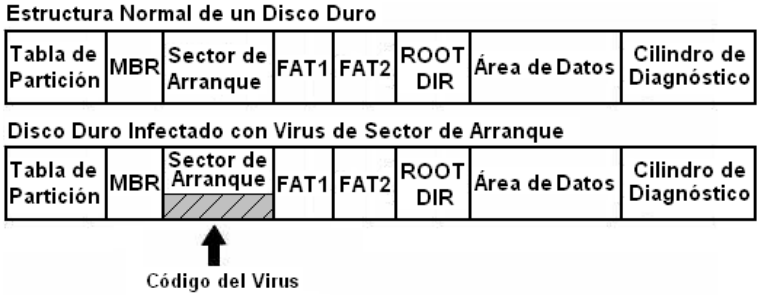


Fig 3.7. Virus de Sector de Arranque.

Un virus de este tipo infecta discos duros o disquetes, para posteriormente cargase en memoria y permanecer residente para tratar de infectar otros dispositivos.

Para que este tipo de virus tengan éxito, se debe cumplir la siguiente secuencia:

1. Un archivo infectado es copiado hacia un disquete desprotegido.
2. El disco es dejado de manera inadvertida durante el inicio del equipo.
3. Durante el inicio, el virus es cargado a la memoria del equipo.

Cuando se intenta iniciar el equipo con un disco infectado, aparece en pantalla el mensaje *"Non system disk or disk error";* mientras el mensaje es mostrado, la infección se lleva a cabo. Cuando el virus es ejecutado, éste infecta el MBR del disco duro y en cada inicio del sistema el virus será cargado en memoria e intentará infectar los disquetes leídos en el equipo. Como ejemplo de este tipo de virus está *"Brain"*, mencionado anteriormente.

Virus de Archivo

En 1986, un programador llamado Ralf Burger se dio cuenta que un archivo podía copiarse a sí mismo, agregando una copia de él a otros archivos. Observando este fenómeno, desarrolló un virus de prueba al que llamó "*VirDem"*, que podía infectar cualquier archivo con extensión *.com*.

En el ambiente DOS[49], cuando se invoca a un archivo para ejecutarlo sin indicar su extensión, el S.O. busca primero el archivo de tipo *.com*, característica que aprovechan los virus de archivo, ya que el virus no modifica el programa original, porque cuando encuentra un archivo *.exe*, crea otro de igual nombre y en el mismo lugar, pero con extensión *.com* que incluye el código del virus.

[49] D.O.S. Disk Operating System, antecedente del Sistema Operativo MS-DOS.

Un virus que infecta archivos *.com* actúa al invocar al archivo, ya que lee primero el encabezado del virus (fig 3.8-1), "salta" el código del archivo original (fig 3.8-2) y ejecuta el código del virus; concluida la ejecución del virus, devuelve el control a la aplicación original (fig 3.8-3), y sigue normalmente.

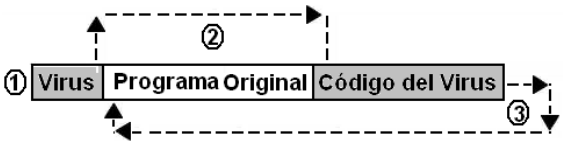


Fig 3.8. Secuencia de Virus en Archivo *.com*

Uno de los primeros métodos de ocultamiento fue utilizado por estos virus: cuando detectan la ejecución del programa antivirus, descargan de la memoria partes de su propio código, y cuando el antivirus finalice la búsqueda, se cargará de nuevo en memoria.

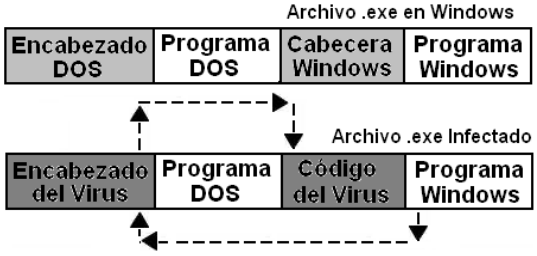


Fig 3.9. Secuencia de Virus en Archivo *.exe*

Los virus de archivos *.com* pueden ser de *Acción Directa*, es decir, que no quedan residentes en memoria y se replican al momento de ejecutar el archivo infectado; y los de *sobrescritura*, o sea, aquellos que corrompen el archivo donde se ubican al sobrescribirlo.

Por su parte, los virus que infectan archivos *.exe*, también tienen un funcionamiento específico. Los archivos *.exe* tienen dos encabezados, de hecho, son dos programas en un mismo archivo, es decir, un programa basado en DOS, y otro que es el archivo en Windows. En cada archivo de Windows existe un encabezado de DOS, un programa basado en DOS y una cabecera. Cuando el archivo es infectado, el virus sustituye la cabecera DOS por su propia cabecera para que "salte" la ejecución del programa y en su lugar se ejecute el código del virus, una vez ejecutado el código del virus, se devuelve el control al programa DOS (fig 3.9), dejando al archivo inutilizable e irrecuperable.

Por esto, se realizaron cambios a la familia Windows, como la introducción del formato de archivo *Portable Ejecutable (PE)*[50], que permite que un archivo se ejecute y se transporte a cualquier equipo con Windows; para guardar compatibilidad con las versiones anteriores, se conservó la cabecera de Windows.

La estructura de los archivos PE es diferente dependiendo del tipo de sistema; por tanto, los virus agregan nuevas cabeceras en la estructura de los archivos. Para mantenerse ocultos, los virus colocan código en áreas vacías del archivo conocidas como "espacios vacíos" (fig 3.10), provocando que el archivo se corrompa.

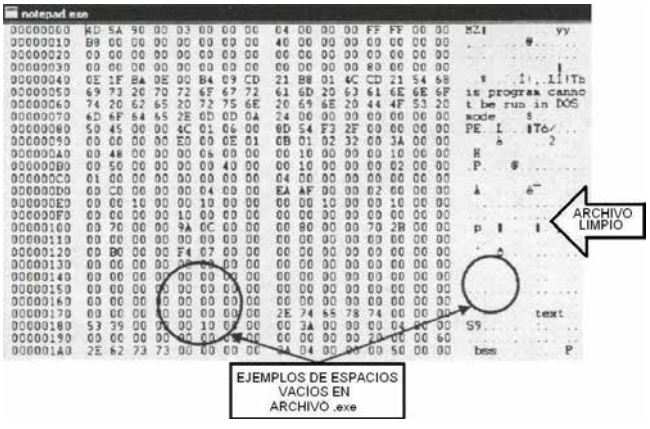


Fig 3.10. Espacios Vacíos en Archivo *.exe*

[50] Especificación derivada de Unix Coff (Common Object File Format).

Virus de Macro

Este tipo de virus se encuentra en archivos que manejan macros[51], ya sea procesador de texto, hoja de cálculo, manejador de presentaciones o de base de datos; así, un *virus de macro*[52] de hoja de cálculo puede infectar un documento elaborado con un procesador de texto y viceversa. Estos virus se alojan también en archivos de aplicaciones y pueden infectar otros archivos u otros S.O.. El código del virus se encuentra dentro del código de la macro y cada que ésta es invocada, el virus se activa.

Los virus de macro, a diferencia de otro tipo de virus, no son exclusivos de algún S.O., y se diseminan fácilmente a través de archivos adjuntos de correo electrónico, unidades removibles, transferencia de archivos, aplicaciones compartidas y demás (fig 3.11).

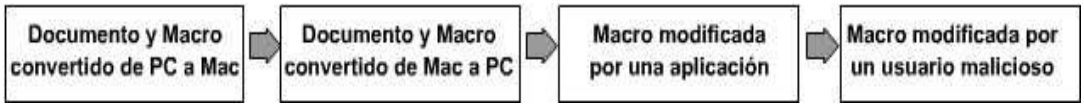


Fig 3.11. Diferentes formas de infección de Virus de Macro

Virus Multipartitas

Este tipo de virus son una combinación de todos los anteriores y pueden infectar sectores de partición y arranque, archivos, y además puede ser activados por medio de macros. Un ejemplo representativo de estos virus es "NATAS" (también conocido como "SATAN"), que en 1994 infectó alrededor del 80% de los equipos de cómputo a nivel mundial[53].

Virus de Red

Son aquellos que se propagan a través de recursos compartidos en red, e-mail o Internet.

Por ejemplo, los applets de JAVA[54] y los controles Active X[55] son lenguajes orientados a Internet, sin embargo, este tipo de códigos no son considerados como virus, porque no tienen la capacidad de replicarse, pero puede contener otro tipo de código malicioso peligroso y de rápida propagación. Los applets de JAVA fueron inicialmente diseñados para correr sólo en un área restringida del sistema llamada "sandbox", pero las restricciones de esa área limitaban las funcionalidades de los applets, por lo que se realizaron cambios en las dimensiones de esta área para implementar funciones como el acceso a archivos.

Los componentes Active X son similares en diseño a un applet, pero permiten efectuar más funciones, como la ejecución de archivos dañinos, lo que puede ser muy riesgoso. Los applets de Java y JavaScript son más comunes que los componentes Active X, pero también pueden contener código malicioso.

[51] Macro: Subrutina que realiza de manera automática algunas tareas rutinarias y repetitivas como cálculos y funciones matemáticas, insertar textos, o presentaciones.

[52] También conocidos como Macro Virus.

[53] Fuente: ICSA. www.icsalabs.com

[54] Programa escrito en lenguaje Java que puede ser incluido en una página HTML para agregarle cierta funcionalidad. El código del applet es transferido a la máquina local y ejecutado por el navegador como Java Virtual Machine (JVM ó Máquina Virtual de Java).

[55] Controles que se pueden implementar en diferentes lenguajes de programación y que se pueden insertar en una web para proporcionar una funcionalidad que no está disponible en HTML.

Por su parte, los virus tipo mIRC[56] aparecieron a finales de 1997. mIRC permite realizar conexiones con servicios de chat y ejecutar automáticamente un script[57], el cual crea otro archivo script que es enviado a todos los usuarios que intenten conectarse al servicio. Así, el virus propagado puede mostrar mensajes en pantalla, robar contraseñas o información confidencial, e incluso, borrar archivos de sistema.

En noviembre de 1998 aparece el *maleware* desarrollado con Visual Basic (VBScript[58]), que fue colocado en sitios de Internet para que al momento de ser accedidos, pudieran propagar el virus; el riesgo, es que pueden infectar diferentes equipos a través de diferentes navegadores de Internet, sobrescribiendo archivos o suplantando a los originales. En 1999, los virus comenzaron a aprovechar el ambiente de red para propagarse, ya que en lugar de infectar un solo equipo o de requerir la intervención del usuario, aprovecharon las vulnerabilidades de algunos programas, como los manejadores de correo electrónico, tal como lo hizo "Melissa".

"Melissa" es un virus de macro para documentos de Word, famoso por su propagación a través de Outlook. Este virus crea un objeto en Outlook usando instrucciones de Visual Basic y accede a la lista de contactos de la libreta de direcciones; luego, crea un mensaje de correo electrónico y se envía a los primeros 50 contactos de la lista junto con un documento infectado (que incluye una lista de páginas pornográficas). "Melissa" cambió la historia, ya que fue tan peligroso, que las compañías antivirus lo clasificaron con el nivel de riesgo *High Outbreak* (descrito en la siguiente sección de este capítulo), lo cual derivó en cambios en los algoritmos de búsqueda de virus.

3.3.3. Morfología

Un virus elemental realiza ciertas acciones específicas: busca un programa, lo infecta y entrega el control al programa infectado. El virus más pequeño en cuanto a código mide solo 45 bytes y en su pseudocódigo[59] se usan las mismas convenciones que usó Fred Cohen en su tesis doctoral *"Computer Viruses",* es decir:

:= se usa para definiciones de programas y subrutinas,
: se usa al final de un nombre para usarlo como etiqueta de una instrucción,
; separa instrucciones,
= asigna valores a las variables y también en las comparaciones;
~ implica negación,
{ , } sirven para agrupar instrucciones

[56] mIRC es un programa que permite hacer conexión a un servicio de Chat ó IRC (Internet Relay Chat).
[57] Archivo con un conjunto de instrucciones que permite automatizar una tarea.
[58] Lenguaje Interpretado en Visual Basic.
[59] Tomado del Libro "virus computacionales" Mallén F. Guillermo M.

```
Programa virus_elemental :=
{
Procedimiento infecta:=
{
        archivo = archivo_ejecutable_elegido_al_azar;
        inserta_virus_al_inicio_del_archivo;
        regresa;
}
Programa_principal:=
{
        Infecta;
        Salta final;
}
final:
}
```

Hasta el año 1990 los virus tuvieron una estructura similar a la anterior, pero ésta ha ido cambiando con el paso del tiempo y con la tecnología; hoy se pueden desarrollar virus con funciones de ocultamiento o dispersión más complejas.

3.3.4. Nomenclatura

Para identificar a un virus se le designa un nombre de acuerdo a tres criterios, según la CARO[60]: una familia, un infijo y un sufijo. De vez en cuando, los nombres de virus difieren de los criterios dependiendo de las características del propio virus.

El primer virus con un determinado conjunto de características que lo identifica como una entidad totalmente nueva y diferente recibe el nombre de "familia", cuyo nombre se establece a partir de una característica anómala en el virus, una cadena de texto, o su efecto. Un nombre de familia puede incluir una cadena numérica que designe el tamaño en bytes del virus, esto se hace para distinguirlo de variantes similares.

Los nombres de las variantes en una familia constan del nombre de familia y un sufijo (por ejemplo: BadVirus.a); para designar ese sufijo se sigue un orden alfabético comenzando con la letra *"a"* hasta llegar a la *"z"*; luego, inicia con *"aa"* y continúa hasta llegar a *"az"*. Las variantes posteriores reciben el sufijo *"ba"* hasta *"bz",* y así sucesivamente, hasta que las designaciones de sufijo alcanzan *"zz";* en el caso que aparezca otra variante, se continuará con *"aaa".*

Al aparecer nuevas cepas[61] de virus, las convenciones de designación de nombres evolucionaron para incluir más información; por ejemplo, algunos nombres incluyen partes que identifican la plataforma en la cual se puede ejecutar el virus. Por otro lado, el prefijo designa el tipo de archivo que es infectado o la plataforma en la que se ejecuta el software dañino. El convenio de denominación incluye los siguientes prefijos:

[60] Computer Anti-virus Research Organization. Grupo que asocia a fabricantes e investigadores de virus a nivel mundial, antecedente de EICAR.

[61] Grupo de organismos emparentados, como las bacterias, los hongos o los virus, cuya ascendencia común es conocida. Fuente: www.rae.es

PREFIJO	CONCEPTO
A97M/	Virus de macro que infecta archivos de Microsoft Access 97.
Bat/	Virus de archivo por lotes. Se ejecuta como archivo *bat* que afecta al programa que interpreta los comandos del archivo por lotes. Se desplaza fácilmente y puede afectar a casi cualquier plataforma que ejecute archivos por lotes
IRC/	Virus de archivo de guión de *Internet Relay Chat*; utiliza versiones antiguas del software cliente de mIRC para la distribución de virus.
JS/	Virus de guión o programa troyano creado en el lenguaje JavaScript.
Linux/	Virus de guión compilado para Linux con el formato de archivo ELF.
MacOS/	Programa troyano para el sistema operativo Apple OS versiones 6-9.
MSIL/	Aplicación creada con *Microsoft Intermediate Language* (plataforma .NET).
PHP/	Virus de guión o programa troyano creado en el lenguaje PHP.
PP97M/	Virus de macro que infecta archivos de Microsoft PowerPoint 97.
SunOS/	Programa potencialmente dañino para Sun Solaris.
Unix/	Programa o guión de shell para UNIX.
VBS/	Virus de guión o programa troyano creado en el lenguaje Visual Basic Script.
W2K/	Programa peligroso para entornos de 32 bits de Win NT, 2000 o XP.
W32/	Virus que infecta archivos o boot sector en entornos de 32 bits de Win 95, 98 o NT
W95/	Virus que infecta archivos y que se ejecuta en entornos Win 95, Win 98 y Win ME.
W97M/	Virus de macro que infecta archivos de Microsoft Word 97.
X97M/	Virus de macro que infecta archivos de Microsoft Excel 97.

Por su parte, el infijo es una designación que aparece normalmente a la mitad de un nombre de virus; entre los principales sufijos se encuentran:

INFIJO	CONCEPTO
.cmp.	Archivo acompañante que el virus agrega a un archivo ejecutable existente; los antivirus eliminan el archivo acompañante para prevenir futuras infecciones.
.mp.	Virus multipartito de DOS.
.ow.	Virus de sobrescritura. Identifica un virus que sobrescribe datos en un archivo, dañándolo irreparablemente. Dicho archivo debe eliminarse.

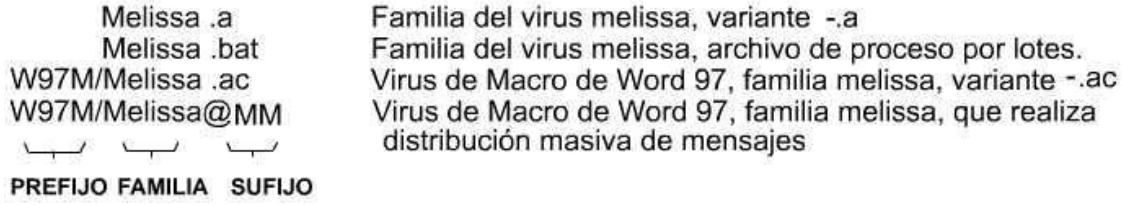
El sufijo es una designación que aparece en la última parte de un nombre de virus. Un virus puede tener más de un sufijo: uno para designar una variante y otro para información adicional. Los sufijos que se utilizan por convención son:

SUFIJO	CONCEPTO
@M	Envío lento de mensajes. Este virus utiliza un sistema de correo electrónico.
@MM	Distribución masiva de mensajes. El virus puede usar técnicas estándar pero también algún sistema de correo electrónico para propagarse.
.a - .zzz	Variantes de virus.

Por convención, los sufijos específicos designados por los fabricantes de antivirus pueden ir precedidos del carácter "**!**". Los sufijos mas utilizados son:

SUFIJO	CONCEPTO
apd	Virus que anexa código al archivo que infecta, no se replica correctamente.
bat	Componente de software en el lenguaje BAT.
cav	Virus de cavidad. Designa un virus que se copia a sí mismo en "cavidades" (por ejemplo, en áreas de sólo ceros) en un archivo de programa.
cfg	Componente de configuración de un programa troyano de Internet (con frecuencia del tipo 'BackDoor').
dam	Archivo dañado. Designa un archivo dañado o corrupto por una infección.
gen	Detección genérica. Las rutinas originales de software antivirus detectan a este tipo de virus sin utilizar cadenas de código específicas.
ini	Guión mIRC o pIRCH que es un componente de otros virus.
intd	Virus "Intencionado". Virus que posee la mayoría de las características más comunes de los virus, pero no se puede replicar correctamente.
irc	Componente IRC de un programa potencialmente dañino.
js	Programa potencialmente dañino creado en JavaScript.
kit	Virus o programa troyano creado con un 'kit de creación de virus'.
p2p	Programa dañino que usa comunicación punto a punto, como Gnutella o Kazaa.
sfx	Utilidad de instalación de auto extracción para programas troyanos
src	Código fuente viral. No puede replicarse ni infectar archivos, pero algunos virus dropper lo incluyen en los archivos como parte del ciclo de infección.
sub	Virus de sustitución. Sustituye al archivo anfitrión, de modo que todos los archivos anfitriones infectados tengan el mismo tamaño.
svr	Servidor de un programa troyano de Internet (con frecuencia del tipo 'BackDoor').
vbs	Componente de un programa dañino creado en el lenguaje Visual Basic Script.

De esta forma, y tomando como ejemplo al virus "Melissa", existen algunas variantes de este virus, cada una con ciertas particularidades en su nomenclatura:



3.3.5. Niveles de Riesgo

Para medir el nivel de riesgo de un virus de manera concreta, se realiza una clasificación, que toma en cuenta las características de los virus según algunos criterios, aunque el más significativo es la *Prevalencia,* concepto que surge en epidemiología médica; en ese contexto, se refiere a la proporción de personas que sufren una enfermedad con respecto al total de la población en estudio.

En cómputo, la ***Prevalencia*** refleja el número de virus descubiertos "en campo"[62] por los investigadores antivirus, es decir, mide qué tan extendido está un virus en un momento determinado. Para una mejora clasificación, existen cuatro niveles de prevalencia:

[62] Hace referencia al ambiente de cómputo cotidiano tanto en organismos públicos como privados.

Muy Extendido. Un virus se ubica en esta clasificación cuando es detectado en un periodo de 4 horas por 20 instancias distintas (empresas privada, públicas, gobiernos, universidades e investigadores de virus alrededor del mundo); la ubicación geográfica de los reportes no es significativa, ya que en un país o región el virus puede estar más difundido que en otro.

Nivel Extendido. En este nivel se ubican los virus detectados por menos de 20 instancias distintas durante un día laboral, los casos reportados pueden ser de uno o varios países.

Nivel Menos Extendido. Incluye a los virus detectados por menos de 20 instancias en un periodo de varios días.
Nivel No Extendido. En esta clasificación se tiene conocimiento de la existencia de algún virus, pero no ha sido reportada ninguna infección porque los virus aquí incluidos no se encuentran en campo.

Por otro lado, la ***Incidencia*** es otro criterio para clasificar a los virus y se refiere al número de equipos infectados en un periodo determinado: horas, días, meses, o cualquier otro.

Un criterio más es el ***Efecto Dañino***, el cual refleja la magnitud del daño resultado de una infección. Para que los daños sean medidos de manera concreta, se definen categorías:

Daño Irrecuperable. Cuando un virus redistribuye datos confidenciales a terceras partes.

Daño Muy Serio. Cuando el virus manipula datos de manera silenciosa o insospechada.

Daño Serio. Cuando un virus borra archivos, formatea discos o borra memorias Flash.

Daño Medio. Cuando el virus borra algunos archivos y deja a la computadora temporalmente no disponible.

Daño Menor. Cuando el virus genera sólo mensajes de texto o sonidos.

El último criterio de clasificación de los virus es el ***Medio de Infección***, es decir, qué tan común es el sistema operativo, programa o ambiente en que el virus actuará; los virus son diseñados para infectar las plataformas o programas más comunes; por ejemplo, es más común encontrar virus para Windows que para Linux o MAC. Así, el medio de infección indica el número de usuarios de computadoras que usan un programa o sistema que un virus puede infectar; se considera que las plataformas y programas comunes dan más oportunidad a la proliferación de virus. Para este criterio se han definido tres niveles:

Nivel Muy Común. Comprende sistemas operativos de uso común, como los de la familia Windows o aplicaciones de Microsoft Office.

Nivel Común. Incluye sistemas operativos de uso poco frecuente como MAC-OS y DOS, o aplicaciones como Java o Visual Basic.

Nivel Poco Común. Considera sistemas operativos de uso limitado como OS/2 ó Unix, o aplicaciones como Access, Corel Draw (Corel Script).

Los criterios anteriores también consideran la posibilidad de que un equipo se encuentre conectado a una red o tenga acceso a Internet, ya que, estos medios son los más utilizados actualmente por los virus, lo que amplía las posibilidades de infección.

De acuerdo a lo anterior, los criterios para evaluar el nivel de riesgo de un virus quedan organizados de acuerdo al siguiente esquema:

De acuerdo a los criterios anteriores, los niveles de riesgo (descritos a continuación) se clasifican de acuerdo al potencial para cada nivel, del más alto al más bajo y mencionando los virus más representativos en cada uno, así como algunas acciones inmediatas para mitigar el efecto infeccioso.

Fuera de Control (High-Outbreak)
Es el nivel más alto dentro de la clasificación de riesgos. Estos virus se propagan en pocas horas a través de correo electrónico masivo; a pesar de las políticas y acciones implementadas para evitar su daño, estos virus salieron de control a las pocas horas de haberse descubierto, por lo tanto, se considera que los virus más malignos se ubican en este nivel, que aunque son pocos, causaron daños catastróficos; entre ellos están W97M/Melissa, VBS/Loveletter, VBS/VBSWG (Anna), W32/Nimda.

Para combatir este tipo de virus, deben tomarse algunas acciones que no son sencillas. Inicialmente debe ponerse en marcha un plan de emergencia, que defina detalladamente la ruta de comunicación entre los distintos departamentos involucrados, así como sus respectivas responsabilidades.

Se debe tener instalado software antivirus en todos y cada uno de los equipos de la organización, y mantenerlo debidamente configurado y actualizado, principalmente en los servidores de correo electrónico, gateway, servidor de archivos y servidores de aplicaciones.

Se debe también, dar seguimiento cabal de las políticas de seguridad y mantenerse al pendiente de cualquier incidente. Este tipo de virus, hacen trabajar horas extras a los encargados de sistemas, porque son muy difíciles de erradicar por su gran expansión y sus efectos. La operación de la organización, en la mayoría de los casos, ha llegado a ser casi nula debido a la imposibilidad de utilizar los recursos informáticos.

Alto Riesgo (High)
Un virus se ubica en esta clasificación cuando ha sido reportado muy frecuentemente en campo, puede causar serios daños o propagarse rápidamente a sistemas operativos y plataformas de uso común.
Si un virus causa daños irrecuperables, puede ser clasificado como de alto riesgo a pesar de que su prevalencia sea poco frecuente. Un virus se clasifica como "Riesgo Medio en Observación" antes de ser clasificado como "Riesgo Alto". Virus como Win95/CIH, W97M/Thus, VBS/Newlove, W32/Naced han sido clasificados en este nivel de riesgo.

Algunas acciones para combatirlos incluyen la implementación de un plan de emergencia, que defina las responsabilidades de las diferentes áreas de la organización, así como mantener actualizado el software antivirus, principalmente en servidores y estaciones de trabajo; además se debe estar pendiente de cualquier posible incidente dentro de la red de la organización.

Riesgo Medio en Observación (Medium On Watch)
Los virus incluidos en esta clasificación pueden ganar prevalencia muy rápidamente; tienen un efecto dañino que puede propagarlos a través de sistemas operativos y plataformas de uso común.

Este nivel de riesgo está diseñado para funcionar como un sistema de alerta temprana, ya que los virus que alcanzan este nivel se encuentran en observación minuciosa y mucho mas exhaustiva que con los virus de clasificaciones mas bajas, ya que pueden convertirse en virus de alto riesgo en poco tiempo.

Con este tipo de virus se inician las acciones definidas en un plan de emergencia, es decir, definir canales de comunicación y responsabilidades entre las áreas de la organización, mantener actualizado el programa antivirus; pero sobre todo, realizar un análisis de riegos que permita determinar qué tan vulnerables son los recursos de cómputo de la organización, y así, implementar medidas que disminuyan el riesgo.

Riesgo Medio (Medium Risk)
Estos virus tienen un efecto muy destructivo y son capaces de infectar y propagarse a través de plataformas de uso común; entre los virus característicos de este nivel se encuentran W32/Ska (Happy99), VBS/Haptime, Backdoor-Sub7 e W/32Hybris. Se deben seguir las acciones indicadas en un plan de acción para eliminar el virus, así como mantener actualizado el programa antivirus.

Bajo Perfil (Low-Profiled)
Este tipo de virus aparentan ser de "riesgo bajo" porque no tienen un efecto peligroso, pero ameritan un seguimiento mayor, ya que puede aumentar su prevalencia y alcanzar el nivel de "riesgo medio". Este nivel está diseñado solo como prevención, ya que los virus aquí incluidos son de riesgo bajo pero pertenecen a una familia que tienen una alta prevalencia, como "VBS/Bubbleboy", "PalmOS/Phage.963" o W32/Zoher@MM. Para eliminarlos no es necesario realizar alguna acción específica, solo actualizar el programa antivirus de manera regular.

Riesgo Bajo (Low Risk)
Estos virus no se han detectado en campo ni tienen efecto dañino, no tienen un objetivo específico, ni se propagan a sistemas de uso común, pero su efecto es muy serio o irrecuperable.
Ejemplo de ellos son: W97M/JulyKill, VBS/Anjulie y W32/Shoho. No se necesitan tomar acciones adicionales, solo mantener actualizado el programa antivirus.

N/A (No Aplicable)
Este nivel de riesgo se usa en casos donde no existe una infección real, como en los hoaxes. En la descripción de una familia de virus y programas troyanos en general se utilizará el nivel de riesgo N/A porque no se trata de un problema específico.

En general, el nivel de riesgo de un virus puede variar desde el nivel mas bajo, pasar por todas las clasificaciones hasta llegar al nivel más alto en un periodo muy corto si su prevalencia se incrementa; en la mayoría de los casos, un virus en el "Nivel Medio en Observación" aumenta a "Nivel Alto".

El nivel de riesgo también puede bajar si la prevalencia disminuye: cuando un virus ya no es clasificado como de "Alto Riesgo", entra en la categoría "Medio" por un periodo, hasta que vuelve a reclasificarse, generalmente a la baja.

3.4 Gusanos

Un gusano es un programa que se copia a sí mismo en equipos remotos a través de la red, se enfoca a explotar vulnerabilidades encontradas en los sistemas y a recolectar información (contraseñas y archivos) del equipo infectado; también puede dejar una "puerta trasera"[63] y enviarse mediante recursos compartidos, mensajería instantánea, transferencia de archivo IRC, FTP y SMTP.

Los gusanos surgen a finales de los años 70's, cuando los investigadores John Shoch y Jon Hupp del *Centro de Investigación Xerox de Palo Alto*[64], California, idearon un programa que se encargara de las labores de mantenimiento y administración de los equipos de cómputo, al que dieron el nombre de "gusano vampiro".

[63] Puerta Trasera: También conocida como "backdoor". Consiste en aprovechar una vulnerabilidad y dejar abierto el acceso remoto a un equipo para acceder a él, tomar el control del mismo y robar información.
[64] También conocido como Palo Alto Research Center (*PARC*)

El nombre fue tomado de una novela de ficción llamada "*The Shockwave Rider*", en la que un programa llamado "*gusano*" se reproducía hasta el infinito y no podía ser eliminado. El gusano "dormía" por el día y por la noche se propagaba por todas las computadoras del centro.

Dos días después de haber sido creado, el gusano escapó de los equipos de prueba y se extendió por toda la red, paralizando los equipos y colapsando la red. Al intentar eliminarlo seguía reapareciendo, por lo que tuvieron que crear otro programa que fuera por todas las máquinas “matando” copias del gusano, lo que se considera como el antecedente de los antivirus actuales.

En 1980, la red ARPANET se infectó y quedó fuera de servicio por 72 horas a causa de un "gusano" propagado por un estudiante. En mayo de 2000 apareció “VBS/Loveletter” (también conocido como "ILOVEYOU"), el gusano con mayor velocidad de propagación de la historia, el cual fue creado en el lenguaje VBS (Visual Basic Script) y se envía por IRC y correo electrónico en un mensaje con el asunto: "ILOVEYOU".
Loveletter utiliza la libreta de direcciones de Outlook para reenviarse a todos los contactos, provocando que más de 3 millones de equipos fueran infectados, causando pérdidas que superaron los 2.000 millones de dólares en todo el mundo.

3.5 Caballos de Troya

Los caballos de Troya son programas cuyo código malicioso se oculta en programas aparentemente no dañinos (como fotos, videos, documentos, entre otros) y su único propósito es completar una tarea específica, más que replicarse. Se instalan en el sistema al ejecutar el archivo que los contiene, luego, parecen realizar una función útil, aunque internamente realizan otras tareas de las que el usuario no es consciente.

Por ejemplo, pueden recolectar información, contraseñas y archivos del equipo infectado; además, dejan una “puerta trasera” para obtener acceso remoto al equipo. Los programas troyanos (como son más conocidos), pueden causar el mismo daño que un virus.

Su nombre fue tomado del mítico caballo de madera que los griegos obsequiaron a los troyanos, porque estos programas dan una apariencia inocente por fuera, aunque no se sabe qué contienen por dentro; son casi como un kamikaze, ya que tratará de completar la tarea asignada a pesar de que pueda destruirse él mismo.

Un ejemplo característico de un caballo de Troya es, precisamente, “APS trojan” (AOL paswword stealing), código malicioso que se instala en el equipo y roba contraseñas de los usuarios de la compañía America On Line (AOL).

En la nomenclatura para los caballos de Troya, los prefijos también tienen convenciones: el nombre de clase va seguido de caracteres adicionales para indicar una familia (por ejemplo, BackDoor-JZ) o un nombre (como BackDoor-Sub7). A continuación se listan los prefijos más comunes:

PREFIJO	CONCEPTO
AdClicker	Accede de forma repetida a sitios Web que se financian por publicidad.
Adware	Instala programas de publicidad sin autorización del usuario.
BackDoor	Ofrece acceso o control remotos por Internet o por red.
Dialer	Marca un número de teléfono sin el consentimiento del usuario.
DDoS	Componente de Denegación de Servicio Distribuido (DDoS).
Del	Elimina archivos.
Downloader	Descarga software desde Internet, normalmente backdoor, para recolectar contraseñas, archivos y, a veces, virus.
Exploit	Explota una vulnerabilidad o defecto de un programa.
FDoS	Indica un componente de ataque masivo de denegación de servicio
KeyLog	Registra pulsaciones del teclado para transmitirlas al atacante.
Kit	Indica un programa diseñado para crear un virus o programa troyano.
MultiDropper	Libera varios programas troyanos o virus ('backdoors') diferentes.
Nuke	Utiliza defectos del software en un equipo remoto para detenerlo.
ProcKill	Finaliza los procesos de los productos antivirus y de seguridad. También puede eliminar archivos asociados con dichas aplicaciones.
PWS	Roba contraseñas.
Reboot	Reinicia el equipo.
Reg	Modifica el registro de forma no deseada sin el consentimiento del usuario: Reduce la configuración de seguridad o crea asociaciones irregulares.
Spam	Actúa como una herramienta para correo no deseado.
Spyware	Controla los hábitos de navegación y otros comportamientos; envía esta información a otros destinos para publicidad no solicitada.
Uploader	Envía archivos y otros datos desde el equipo.
Vtool	Indica un programa utilizado por los creadores de virus y piratas informáticos para el desarrollo de programas.
Zap	Elimina de forma permanente todo o parte de un disco duro.

3.6 Bromas (Jokes)

Los jokes son programas que aparentan contener código malicioso y de realizar alguna acción dañina en el equipo; no son virus reales, sino simples bromas que buscan preocupar al usuario, haciéndole creer que una acción específica es provocada por efecto de un supuesto virus. Para una víctima de estas bromas, es difícil mantener la calma, sobre todo mientras aparece una ventana en su monitor mostrando cómo se formatea su disco duro o cómo se borran sus archivos; al final aparece algún mensaje indicando que todo se trató de una broma.

Son famosos algunos jokes por su originalidad o por su simpatía, otros por ser groseros o de mal gusto, y aunque en general, no tienen un efecto dañino, provocan una baja en el desempeño laboral.

3.7 Engaños (Hoaxes)

Los hoaxes son mensajes distribuidos por correo electrónico que aprovechan la ignorancia de los usuarios, haciéndoles llegar una supuesta alerta de un nuevo virus muy dañino; al mismo tiempo, realizan supuestas recomendaciones para evitar la infección. También sugieren retransmitir la alerta a todos los usuarios posibles, lo que agrega carga de trabajo al servidor de correo electrónico y aumenta el consumo del ancho de banda.

Y aunque en realidad no son virus verdaderos, los hoaxes llegan a causar pánico y desconcierto entre los usuarios y afectar el rendimiento laboral.

Algunos hoaxes solicitan reenviar un correo electrónico a cuantos contactos sea posible, y por cada mensaje, la compañía *patrocinadora* le hará llegar al remitente cierta cantidad de dinero; otros notifican al usuario que ha sido ganador de un viaje o una cantidad millonaria.

Fig 3.12. Imagen de "BugBear"

Un hoax muy famoso es "bugBear"; consiste en un mensaje que llega por correo electrónico indicando que un archivos de Windows está infectado y debe ser borrado; el archivo en referencia es *jdbgmgr.exe*[65] ubicado en carpeta c:\windows\system; este archivo es una utilería para el navegador Internet Explorer. Cuando el usuario busca el archivo, éste se encuentra, y además tiene asignado el icono de un oso (fig 3.12), con lo que crece la confusión.

El hoax solicita borrar el archivo y reiniciar el equipo; la conexión a Internet no puede completarse, ya que algunas funciones del navegador estarán inactivas. Desafortunadamente, este mensaje llegó (y sigue llegando) a miles de usuarios de cómputo; la mayoría cayeron en el engaño, con lo que muchos equipos quedaron sin conexión a Internet, con las consecuencias que esto representa.

En general, el código malicioso ha evolucionado a lo largo del tiempo, su principal motor de cambio es la tecnología. Debido a este fenómeno, los programas antivirus tradicionales solo ofrecen protección contra el código malicioso revisado hasta esta sección, ya que el código malicioso surgido recientemente rebasa, por mucho, las funciones asignadas a un programa antivirus, por lo que los daños pueden ser imperceptibles durante mucho tiempo, pero sobre todo porque no existe la mínima sospecha de su existencia. Las nuevas formas de código malicioso se describen en las siguientes secciones.

3.8 Programas Espía (Spyware[66])

Los programas espía o spyware son aplicaciones que recopilan información, a través de los sistemas informáticos, sobre una persona u organización sin su conocimiento, para después, distribuirla a empresas publicitarias u otras organizaciones que lucran con dicha información. Estos programas registran y envían información respecto a hábitos de navegación en Internet y datos relativos al equipo afectado: sistema operativo, tipo de procesador y memoria; aunque también se han empleado en círculos legales para recopilar información contra sospechosos de delitos.

Los programas espía pueden ser instalados en una computadora por medio de un virus o un programa troyano que se distribuye por correo electrónico, también puede estar oculto en los archivos de instalación de un programa aparentemente inofensivo; como resultado, comprometen la privacidad y alteran la configuración del equipo afectado.

[65] "Microsoft Debugger Registrar for Java"
[66] Palabra que proviene de la frase en inglés "Spy Softawe".

Así mismo, los programas de recolección de datos instalados con el conocimiento del usuario, no son realmente programas espías si el usuario comprende plenamente qué datos están siendo recopilados y a quién se distribuyen. Ejemplo de ello son las cookies, un mecanismo que almacena información sobre un usuario de Internet en su propio equipo; se suelen emplear para asignar a los visitantes de un sitio de Internet un número de identificación individual para su reconocimiento subsiguiente.

Pero, la existencia de las cookies y su uso generalmente no están ocultos al usuario, quien puede desactivar el acceso a la información de las cookies; el problema aquí, consiste en la desinformación. Dado que un sitio Web puede emplear un identificador cookie para construir un perfil del usuario y éste no conoce la información que se añade a este perfil, se puede considerar a los cookies una forma de spyware.

Por ejemplo, una página con motor de búsqueda puede asignar un número de identificación individual al usuario la primera vez que visita la página, y puede almacenar todos sus términos de búsqueda en una base de datos con su número de identificación como clave en todas sus visitas subsiguientes (hasta que el cookie expira o se borra). Estos datos pueden ser empleados para seleccionar los anuncios publicitarios que se mostrarán al usuario, o pueden ser transmitidos (legal o ilegalmente) a otros sitios u organizaciones.

Detectar spyware en un equipo no es fácil, pues estas aplicaciones utilizan técnicas sofisticadas para pasar desapercibidas, o recurren incluso a técnicas de ocultamiento. Normalmente, el programa espía se instala (de manera oculta) junto con algún otro tipo de aplicación; al no tratarse de virus ni utilizar alguna rutina que pueda relacionarse directamente con ellos, los programas antivirus no resultan efectivos para detectarlos.

El problema es grave; un estudio realizado en noviembre de 2004, estimó que 67% de los equipos de cómputo a nivel mundial se encuentran infectadas con algún tipo de programa espía[67], entre ellos: Magic Lantern (desarrollado por el FBI para recolectar datos y contraseñas de sospechosos), Bonzi Buddy, y Claria Corporation.

3.9 Adaware

Los programas publicitarios o “adaware” son aplicaciones diseñadas para mostrar al usuario publicidad no solicitada, principalmente, anuncios de compañías que obtienen ingresos a través de publicidad por Internet. Los programas adware, no roban información ni espían las actividades del equipo, sin embargo, se instalan en manera oculta, y muy rara vez pueden solicitar permiso para instalarse.

Estos programas muestran mensajes o ventanas intercaladas entre las ventanas de instalación de otros programas legítimos, así, el usuario otorga (inadvertidamente) permiso para instalarlos en su equipo; luego, adaware intenta conectarse a un servidor, que le indica los anuncios a mostrar.

[67] Fuente: http://www.itfacts.biz

Cuando el usuario navega por Internet, se abre una conexión con la máquina remota, para luego mostrar una ventana publicitaria; otras variantes redireccionan la página de inicio o llevan a sitios pornográficos en Internet sin autorización del usuario.

Una tendencia actual consiste en que el adware se instala en combinación con programas espías, que recopilan adicionalmente estadísticas relacionadas con los hábitos de navegación del usuario. De esta manera, se selecciona con mayor precisión el perfil de publicidad que se muestra a cada usuario. Se calcula que este problema se agrava cada día, ya que cualquier equipo conectado a una red puede llegar a tener, por lo menos, 13 programas adaware instalados sin que sus usuarios estén enterados[68].

3.10 Spam

El correo basura, también conocido como "spam", consiste en mensajes comerciales que se distribuyen masivamente a través de Internet, con el fin de promocionar ciertos productos o servicios, como los financieros, ofertas en supermercados, medicamentos "milagro" (como viagra), productos pornográficos, software pirata, entre otros.

El spam es producido por compañías que cobran por enviar mensajes publicitarios masivamente a través de Internet; dichas compañías generan sus listas de destinatarios potenciales mediante el robo o la compra (lícita o ilícita) de grandes bases de datos.

En algunos países donde la legislación es deficiente, se pueden obtener bases de manera ilegítima; en otros países, empresas sin escrúpulos venden su información al mejor postor. Las direcciones de los posibles destinatarios también pueden obtenerse de lugares como USENET[69] e incluso de páginas de Internet personales, mediante la utilización de diversos motores de búsqueda especializados.

Los mensajes spam pueden saturar los servidores de correo electrónico, el buzón del destinatario o la red, provocando que los mensajes legítimos nunca lleguen. De hecho, cuando llegan mensajes spam, el usuario pierde tiempo en eliminarlos, lo que repercute directamente en su desempeño laboral y en las finanzas y la seguridad de la organización.

Según algunos estudios, entre 70 y 80% de los correos que se transmiten por Internet son spam, de manera que una empresa puede llegar a recibir, en promedio, hasta 459 millones 313 mil 447 correos basura al año. Actualmente el 95% de todo el tráfico de correo electrónico consiste en mensajes no solicitados[70]. Las compañías que usan filtros anti-spam en sus servidores de correo, pueden filtrar solamente una porción del mismo, pues los spammers[71] buscan nuevos medios para engañar a los filtros.

El *Commtouch Spam Detection Center*[72], organización capaz de analizar 1,500 millones de mensajes cada mes, detectó tan solo en junio de 2005 la cantidad de 28 millones de

[68] Fuente: Ruben Galicia, Sistemas de Seguridad TI de McAfee, en entrevista para "El Universal On-Line" Lunes 21 de febrero de 2005, Sección de Computación, pp. 1

[69] Servicio de noticias accesado a través de internet o algún servicio en línea, que contiene mas de 14,000 foros o grupos de noticias sobre temas diversos.

[70] Fuente: SpamHaus Project www.spamhaus.org

[71] Así se conoce a las entidades generadores de spam, ya sean personas físicas o compañías.

[72] Compañía proveedora de soluciones de servicios de mensajería y correo electrónico. www.commtouch.com

correos basura al día, lo que equivale a cerca de 1 millón de mensajes diarios. Según observaciones de esta organización, los países líderes en generación de spam son Corea del Sur, China y Estados Unidos, con cerca del 50% de todos los mensajes spam a nivel mundial. El otro 50% se origina en Europa, Taiwán y América Latina (donde los países líderes son México y Brasil).

De hecho, los mensajes spam ya no solo son considerados como mensajes publicitarios de un remitente desconocido, en la actualidad, se considera como spam a los mensajes enviados por amigos o conocidos, donde se solicita reenviar el mensajes a la mayor cantidad de amigos posible (mensajes cadena), o aquellos que incluyen presentaciones, fotos, chistes u otro contenido no solicitado.

3.11 Phishing

"Phishing" es una variación de la palabra anglosajona *fishing*, que en español significa "ir de pesca". El término se refiere al envío masivo de mensajes electrónicos apócrifos, que fingen ser comunicados oficiales, normalmente de una entidad bancaria o comercial. Su objetivo es recabar información confidencial del usuario, como datos de su tarjeta de crédito o contraseñas, y utilizarlos para realizar un fraude por Internet.
En un mensaje phising, el usuario recibe en su correo electrónico un formulario (apócrifo) donde se le solicitan datos personales, como tarjeta de crédito, contraseñas y demás información confidencial; dicho formulario es una copia idéntica del formulario que se encuentra en el sitio original del proveedor; con que el usuario no nota la diferencia y es víctima del engaño.

Recientemente se realizó un ataque en perjuicio de una institución financiera mexicana, a cuyos usuarios se les intentó engañar con un ataque phising. El día 9 de Febrero de 2005, la compañía Web Sense Security Labs[73], reportó dicho ataque, sin dar a conocer sus alcances o consecuencias. La alerta tenía la siguiente redacción:[74]

Hemos recibido varios reportes de un nuevo ataque phising dirigido a los clientes de la página de Banamex/BancaNet. El ataque, que se hace pasar un correo del "Departamento de Validación" de Banamex, intenta engañar a los usuarios para que visiten una página de Internet fraudulenta. El mensaje es escrito en español y aparece mas abajo. Una vez que los usuarios visitan la página fraudulenta, se les pide ingresar su nombre de usuario y contraseña. Una vez que la información es enviada, el servidor reenvía la información (login.php) a otra página fraudulenta hospedada en Bulgaria.

El primer servidor está hospedado en los Estados Unidos y estaba en línea al momento de emitir esta alerta. El cuerpo del mensaje es el siguiente:

---

[73] Organización dedicada a monitorear y reportar ataques a través de Internet
[74] Fuente: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=132

Estimado cliente de Banamex
Durante nuestro programado mantenimiento regular y procesos de verificación, hemos detectado un error en la información que tenemos registrada de su cuenta.

Esto se debe a algunos de estos factores:

1. Un cambio reciente en su información personal.
2. Que se haya proporcionado información invalida durante su proceso inicial de registro con bancanet o que usted aun no haya realizado dicho registro.
3. La inhabilidad de verificar con exactitud la opción de su elección concerniente a su forma preferente de pago y manejo de cuenta debido a un error técnico interno dentro de nuestros servidores al momento del registro.

Favor de actualizar y verificar la información de su cuenta haciendo clic en la siguiente liga. Será redirigido a la página principal de nuestro sitio en Internet donde podrá actualizar su información personal.

<URL Removida>

Si la información en su cuenta no se actualiza en las siguientes 48 horas algunos servicios en el uso y acceso de su cuenta serán restringidos hasta que esta infamación sea verificada y actualizada. De antemano agradezco su pronta atención este asunto.

Departamento de Validación"D.R. © Copyright 2005, Derechos Reservados.
Banco Nacional de México, S.A., integrante de Grupo Financiero Banamex.
Isabel la Católica 44. Col. Centro Histórico. Del. Cuauhtémoc. C.P. 06000, México, Distrito Federal, México

Para garantizar que el ataque sea exitoso, la página fraudulenta muestra un entorno idéntico a la página original de Banamex, como se muestra (fig. 3.13):

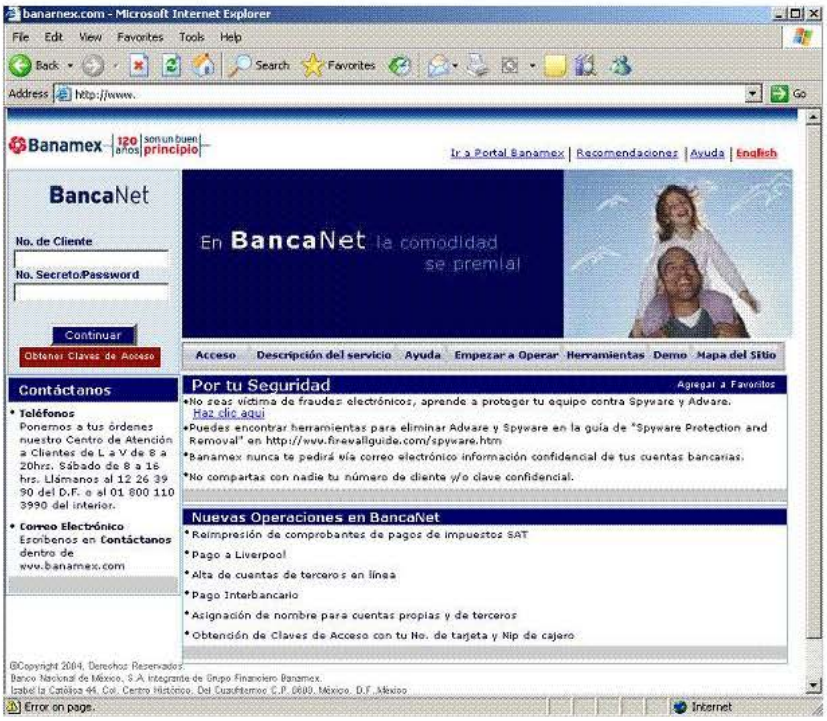


Fig 3.13. Página Fraudulenta

Desafortunadamente, para un usuario tradicional, no es fácil detectar el engaño, sin embargo, existen medidas que se pueden tomar para evitar caer en este tipo de fraudes:

1. En lugar del icono de seguridad en la barra inferior del navegador, se muestra un mensaje de *"Error on Page"* (fig 3.13). Como se había mencionado en el capítulo 2, el ícono de seguridad muestra el certificado digital emitido por una autoridad certificadora, y autentica la validez de la página.
2. Al abrir la página apócrifa, el navegador mostrará una dirección distinta a la dirección original de Banamex.
3. Banamex maneja el protocolo https[75], el cual es mostrado en la dirección URL del navegador (fig. 3.14).

Es importante mencionar que ningún proveedor, ya sea una institución financiera, comercial u otro, no solicitará datos a través de correo electrónico, mucho menos datos confidenciales. En la página auténtica, se muestra el icono de seguridad, y por lo tanto, el certificado digital (fig 3.15).

Por su parte, Banamex, decidió implementar medidas de seguridad adicionales en su sitio, como contraseñas OTP y llaves mas grandes; además recomiendan no utilizar sitios públicos para acceder al portal y no usar ligas para entrar al servicio, sino teclear la información completa en la barra de direcciones del navegador.

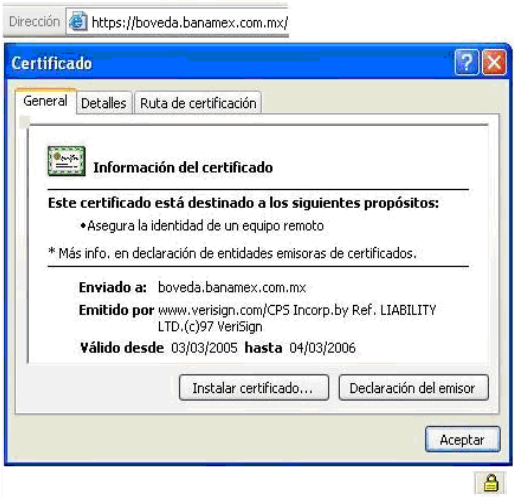


Fig3.14. Certificado Digital Válido

En México, diariamente se reciben 5.7 nuevos ataques phishing. Hacia noviembre de 2004 existían mil 518 sitios de phising, de 51 marcas diferentes, 75% del sector financiero y 16% de los proveedores de servicios de Internet ISP[76].

Asimismo, de acuerdo con un estudio publicado por los Servicios de Inteligencia para la Seguridad de IBM, "Informe de las Tendencias sobre Amenazas y Ataques a la Seguridad", el phishing es la amenaza informática que más rápidamente creció: 5,000% en 2004 [77]. Algunos estudios, como el realizado por Anti-Phisinh Workimg Group[78], dan a conocer que México ha aportado el 0.29% de ataques phising a nivel mundial durante los últimos 12 meses, siendo, Estados Unidos (25.93%), China (17.12%) y Brasil (3.71%) los paises con el mayor porcentaje de ataques.

[75] Hace referencia al protcolo http seguro.
[76] IDEM 43
[77] Fuente: http://www.ibm.com/mx/press/news/2004/11/news_sv_08112004.phtml
[78] Asociación enfocada a prevenir, eliminar y notificar los fraudes y el robo de identidad a través de Internet. www.antiphishing.com

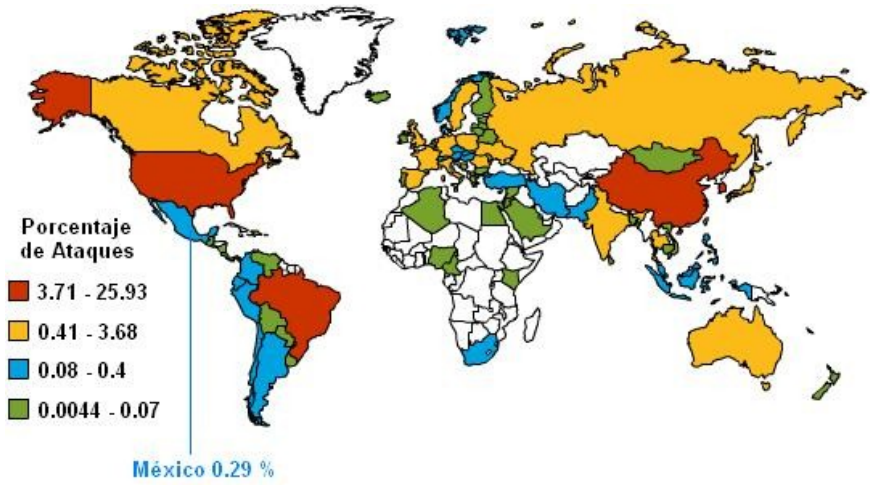


Fig 3.15 Ataques Phising reportados en el último año

3.12 Pharming

Los ataques phishing están evolucionando con rapidez; ahora los estafadores utilizan nuevas técnicas para redireccionar a los usuarios hacia sitios de Internet falsos. Esta nueva modalidad de fraude se conoce como "pharming", que es la explotación de una vulnerabilidad en el servidor DNS[79] que permite a un atacante obtener el *Nombre de Dominio* de un sitio en Internet y redireccionar el tráfico hacia una dirección falsa.

"Pharming" es un nombre simple de un concepto relativamente viejo conocido como "*domain spoofing*" o "*suplantación de dominio*" y es más peligrosa que el phishing. Si el servidor en Internet real recibe una petición, el tráfico se redirecciona hacia una dirección falsa, que puede ser la de un banco, por ejemplo, para robar contraseñas o datos confidenciales relacionados con la pagina original.

Este tipo de ataque solo es posible cuando la página no tiene transacciones protegidas mediante algún mecanismo de seguridad o cuando el usuario ignora las medidas de seguridad sobre certificados digitales, su validez y uso.

Los conocidos "pharmers[80]" trabajan de manera oculta, tratando de "envenenar" el servidor DNS local, redireccionando las peticiones a alguien mas. En cuanto a los navegadores que solicitan información a ese DNS, serán conectados a la página verdadera, pero su información será enviada también al atacante; a través de este método el usuario no necesita contestar un correo electrónico para proporcionar (de manera involuntaria) sus datos a través de Internet.

Para entender de manera más amplia este tipo de ataque, se necesita conocer el funcionamiento del sistema DNS, el cual se explica a continuación:

Cuando un usuario solicita acceso a una página de Internet, una serie de DNS resuelven la dirección tecleada y la "traducen" al binario; estos servidores son básicamente una lista

[79] DNS o Domain Name Server, Servidor de Nombres de Dominio. Se refiere al equipo responsable de resolver los nombres de las direcciones de Internet a su direccion real.

[80] Atacante que realiza ataques Pharming.

de directorios de nombres comunes, como *www.unam.mx*, *www.empresa.com.mx* y una dirección binaria específica que no es visible a simple vista. Cuando se hace una petición a la página *www.unam.mx*, se direcciona hacia el servidor DNS más cercano, el cual localiza la dirección de Internet registrada para el servidor de Internet correspondiente. Para los usuarios, es más fácil recordar la dirección *www.unam.mx* que la dirección binaria 132.248.10.7. Sin embargo, si el ataque va dirigido a la página de la UNAM, la petición del usuario puede ser direccionada hacia una página fraudulenta en Internet.

El ataque pharming también puede ser provocado por la implementación de IDN[81], que permite usar caracteres internacionales en nombres de dominio (como los usados en el idioma japonés o coreano) que reensamblan otros caracteres usados comúnmente (en código ASCII[82]), haciendo creer al usuario que está en un sitio confiable.
Algunos fabricantes de navegadores, como Firefox, han deshabilitado el soporte para IDN como una defensa ante el phising; otro caso es la barra de Netcraft, que al momento de ingresar a un sitio verifica si este no puede ser de procedencia dudosa, advirtiendo al usuario. Sin embargo, la solución para este grave problema son, al igual que en el ataque phishing, los certificados digitales.

Así concluye este capítulo, donde se han revisado las formas de ataque a través de código malicioso, desde las tradicionales hasta las mas nuevas, dando algunos antecedentes y formas de actuar de cada una de ellas, las medidas de prevención se explicarán mas a detalle en el Capítulo 5 “Buenas Prácticas”. En el siguiente capítulo se describen las diversas formas de detección de código malicioso, principalmente las funcionalidades de un programa antivirus.

[81] International Domain Name
[82] American Standard Code for Information Interchange. Código que se utiliza como norma para representar caracteres, generalmente se utilizan 8 caracteres binarios para un caracteres hexadecimal.

4

PROGRAMAS ANTIVIRUS

El presente capítulo muestra las funcionalidades de un antivirus, las técnicas para detectar código malicioso y presenta, además, el cálculo estimado del costo de un ataque.

4.1 Antecedentes.

Cuando los virus informáticos aparecieron a principios de los años 80's, se convirtieron rápidamente en una seria amenaza para las organizaciones debido a la pérdida de productividad y los altos costos que implicaban. Cuando los primeros ataques de virus comenzaron a hacerse públicos, el pánico invadió a muchos usuarios, administradores y organizaciones, situación que aprovecharían algunas empresas para ofrecer sus servicios como asesores de seguridad, y vender programas para detectar y eliminar virus. Este hecho fue el detonador para el surgimiento de la creciente "Industria Antivirus".

4.2 Estructura de un Programa Antivirus.

Un antivirus es un programa que sirve para buscar código malicioso en dispositivos de almacenamiento (discos duros y dispositivos removibles); está compuesto por dos módulos principales, conocidos como *Modulo de Control* y *Modulo de Respuesta.*

El *Módulo de Control* realiza una verificación de integridad en los archivos ejecutables y en las zonas críticas del disco duro (sectores de arranque y partición) limitando la acción de un programa, restringiendo la escritura y registrando los cambios en dichos sectores; también efectúa la identificación de virus mediante diversas técnicas (detalladas en la sección 4.2.1). Por su parte, el *Módulo de Respuesta* es como una alarma que detiene cualquier acción del sistema ante una sospecha de virus.

Los programas antivirus incorporan mecanismos que ayudan a detectar, eliminar y prevenir virus mediante programas residentes, que alertan al usuario sobre accesos no autorizados a la memoria o al disco. Estos mecanismos verifican la memoria RAM, luego las zonas críticas del disco y los archivos almacenados.

4.2.1 Técnicas de detección.

Las técnicas de detección de virus han evolucionado a lo largo del tiempo, paralelamente con las técnicas de infección empleadas por los virus; a continuación se mencionan las mas importantes:

Verificación de Integridad

Este método es conocido también como CRC[83] y consiste en analizar cada archivo comparando su tamaño y la última fecha de acceso. Si alguno de estos datos cambia desde la última vez que el antivirus revisó el archivo, se inicia entonces una exploración.

El uso de esta técnica implica una alta demanda de recursos, ya que todos los archivos deben ser verificados; además, la mayoría de los virus no son detectados mediante verificación de integridad debido a su habilidad para modificar y ocultar los datos verdaderos de un archivo, como su fecha o tamaño.

[83] CRC ó Código de Redundancia Cíclica. Consiste en verificar el número de bytes que forman un archivo, sumarlos y al final agregar el resultado como método para comprobar que el archivo ha sido transferido sin alteraciones.

Por ello, un sistema antivirus debe estar compuesto por un programa detector de virus residente en memoria y otro que verifique la integridad de los sectores de discos duros y archivos ejecutables. Actualmente, los antivirus comerciales cubren ambos aspectos.

Monitoreo de Interrupciones

Para comprender la forma en que funciona este método, es importante detallar algunos conceptos. Así, un *programa* es un conjunto de archivos alojados en disco duro, cuando dicho programa es cargado en memoria se convierte en un *proceso;* por lo tanto, un *proceso* es un *programa* que está en ejecución.

Para que la computadora funcione adecuadamente, el Sistema Operativo administra los recursos de la misma (memoria, hardware y software); particularmente, para la administración de memoria se utilizan métodos basados en el uso de interrupciones[84], las cuales asignan un tiempo a cada proceso de acuerdo a su prioridad, tamaño, u orden en que solicita ser cargado. Cuando se interrumpe un proceso, se debe garantizar que éste se reanude en el mismo estado en el que fue interrumpido; para lograrlo, la información relativa al mismo se almacena en un arreglo de estructuras llamada "*tabla de procesos",* lo que evita que procesos de varios MegaBytes (MB) de tamaño saturen la memoria, y al mismo tiempo, se da oportunidad a procesos más pequeños a ser atendidos.

El método de Monitoreo de Interrupciones es utilizado tanto por los programas antivirus como por los propios virus. En el caso de los antivirus, utilizan este método para identificar las llamadas al sistema, sobre todo después de la ejecución de un virus, con el fin de descargarlo de la memoria y deshabilitarlo, para luego removerlo del archivo que lo aloja.

Por su parte, los virus utilizan esta técnica para interceptar las interrupciones del sistema operativo y el BIOS, de modo que cuando algún programa de seguridad (firewall, antivirus u otro) intente ser cargado en memoria, éste sea deshabilitado, permitiendo al virus realizar su efecto nocivo. Algunos virus quedan residentes con el fin de infectar un archivo cuando éste sea cargado en memoria, como Dark Avenger" o "Rogue II" que utilizan estas técnicas para monitorear las interrupciones utilizadas por el antivirus, desactivarlas, y luego acceder a los servicios del S.O. y del BIOS y tomar absoluto control del sistema.

Otros virus contienen programas que detectan, terminan o deshabilitan software de seguridad, como el gusano "Avril.B" (desarrollado en Visual C++), como se muestra:

//<----------AntivirusNull_Process---------->

```
char* bad_windows_list[BW_TOTAL] = {"Norton","AVP","Anti","Virus","McAfee","anti","virus"};
char* Extensions[TOTAL_EXT] = {".DBX",".MBX",".WAB",".HTML",".EML",".HTM",".IDX",".SHTML",".NCH"};
char* bad_processes_list[BP_ROWS][BP_COLS] = {

{"AVP32.EXE","AVPMON.EXE","ZONEALARM.EXE","VSHWIN32.EXE","VET95.EXE","TBSCAN.EXE","SERV95.EXE"},{"SCAN32.EXE","RAV7.EXE","NAVW.EXE","OUTPOST.EXE","NMAIN.EXE","NAVNT.EXE","MPFTRAY.EXE"},{"LOCKDOWN2000.EXE","ICSSUPPNT.EXE","ICLOAD95.EXE","IAMAPP.EXE","FINDVIRU.EXE","FAGNT95.EXE","DV95.EXE"},{"DV95_O.EXE","CLAW95CT.EXE","CFIAUDIT.EXE","AVWUPD32.EXE","AVPTC32.EXE","_AVP32.EXE","AVGCTRL.EXE"},{"APVXDWIN.EXE","_AVPCC.EXE",
```

[84] También conocidas como IRQ ó Interruption ReQuest o llamadas al sistema.

"AVPCC.EXE","WFINDV32.EXE","VSECOMR.EXE","TDS2NT.EXE","SWEEP95.EXE"},{"SCRSCAN.EXE","SAFEWEB.EXE","PERSFW.EXE","NAVSCHED.EXE","NVC95.EXE","NISUM.EXE","NAVLU32.EXE"},{"MOOLIVE.EXE","JED.EXE","ICSUPP95.EXE","IBMAVSP.EXE","FRW.EXE","FSTOPW.EXE","ESPWATCH.EXE"},{"DVP95.EXE","CLAW95.EXE","CFIADMIN.EXE","AVWIN95.EXE","AVPM.EXE","AVP.EXE","AVE32.EXE"},{"ANTITROJAN.EXE","WEBSCAN.EXE","WEBSCANX.EXE","VSSCAN40.EXE","TDS298.EXE","SPHINX.EXE","SCANPM.EXE"},{"RESCUE.EXE","PCFWALLICON.EXE","PAVCL.EXE","NUPGRADE.EXE","NAVWNT.EXE","NAVAPW32.EXE","LUALL.EXE"},{"IOMON98.EXE","ICMOON.EXE","IBMASN.EXE","FPROT.EXE","FPROT95.EXE","ESAFE.EXE","CLEANER3.EXE"},{"EFINET32.EXE","BLACKICE.EXE","AVSCHED32.EXE","AVPDOS32.EXE","AVPNT.EXE","AVCONSOL.EXE","ACKWIN32.EXE"},{"VSSTAT.EXE","VETTRAY.EXE","TCA.EXE","SMC.EXE","SCAN95.EXE","RAV7WIN.EXE","PCCWIN98.EXE"},{"PADMIN.EXE","NORMIST.EXE","NAVW32.EXE","N32SCAN.EXE","LOOKOUT.EXE","IFACE.EXE","ICLOADNT.EXE"},{"IAMSERV.EXE","FPWIN.EXE","FPROT.EXE","ECENGINE.EXE","CLEANER.EXE","CFIND.EXE","BLACKD.EXE"},{"AVPUPD.EXE","AVKSERV.EXE","AUTODOWN.EXE","_AVPM.EXE","AVPM.EXE","KPFW32.EXE","KPF.EXE"}};

Puede observarse que los programas de seguridad más comunes son incluidos en el código del virus, para que al ser detectados se deshabiliten y ello permita alargar el ciclo de vida del virus. Sin embargo, a pesar de ser muy útil, el uso de esta técnica puede producir un número significativo de “falsos positivos” o “falsos negativos”[85] .

Chequeo de Memoria

Esta técnica se basa en la búsqueda de cadenas de código de virus mientras éste se encuentra cargado en memoria; y aunque puede llegar a requerir muchos recursos o interferir con la ejecución de operaciones válidas, evita el contagio de entidades ejecutables y previene que la infección se expanda más allá de un ámbito fijo, por ello es muy útil y eficiente.

Firmas de Virus

Cuando un virus es desensamblado, es decir, analizado su código fuente, se puede observar que contiene cadenas de caracteres que lo identifican de los demás virus (de manera análoga a la firma autógrafa). Estas cadenas son conocidas como *Firmas de Virus* y son importantes para que el antivirus pueda detectar virus y eliminarlos. Así, los programas antivirus incorporan un archivo denominado "archivo de firmas" o “archivo de definiciones” en el que guardan las cadenas (en formato hexadecimal) correspondientes a cada virus, para que, cuando el antivirus detecte alguna de estas cadenas, el virus sea detectado, deshabilitado y limpiado.

La secuencia muestra cadenas (en hexadecimal) del virus VBS/Loveletter:

134 178 156 177 9 51 219 241 94 28 193 220 123 86 193 214
121 71 232 193 178 50 157 76 9 177 143 178 13 152 153 147
13 55 142 176 95 118 192 176 73 122 192 177 66 125 137 143
69 103 192 199 235 49 141 163 196 63 6 85 231 198 113 62
236 223 122 69 241 197 249 6 35 204 141 183 13 56 193 252
91 118 160 255 72 103 217 246 95 59 223 246 74 97 216 253
94 27 136 251 89 126 193 155 3 96 221 225 72 114 201 231
66 118 192 242 68 127 165 190 143 57 136 157 122 92 255 222
13 51 140 179 25 125 138
10643 256 10425 VBS/LoveLetter

[85] Términos definidos en la sección 4.2.2

Así, el "archivo de definiciones" es una gran base de datos que incluye las firmas de todos los virus conocidos hasta cierto momento, por eso, la lista crece conforme se agregan "firmas" de nuevos virus. Los fabricantes antivirus actualizan los "archivos de definiciones", generalmente, los miércoles de cada semana, excepto cuando se trata de virus de riesgo considerable, en cuyo caso, las definiciones pueden actualizarse en cualquier momento.

Para encontrar virus mediante esta técnica, se analizan todos los archivos, verificando si alguno contiene la cadena específica; si esto ocurre, el antivirus emitirá una alerta indicando que está infectado e intentará limpiarlo; caso contrario, si un archivo no contiene alguna de estas cadenas, se considera limpio. Pero, la protección que ofrece esta técnica (conocida también como "scanning"[86]), es *a posteriori,* ya que si la "firma" de un virus no se encuentra en el archivo de definiciones, éste no será detectado y pasará desapercibido.

Para que la firma de un virus se incluya en el archivo de definiciones es necesario que el virus se analice en laboratorio, luego se deberá extraer el trozo de código que identifica al virus e incluirlo en la próxima versión del "archivo de definiciones". Inicialmente, este proceso podía llevar semanas o meses; en la actualidad puede realizarse en horas (incluso minutos) gracias a que muchas organizaciones alrededor del mundo realizan investigaciones y emiten alertas sobre la presencia de nuevos virus.

Sin embargo, como este método consiste en una sucesión prácticamente infinita de soluciones parciales momentáneas, se considera como una técnica altamente ineficiente, pero se sigue utilizando gracias a que identifica rápidamente la presencia de virus ya conocidos. Así, debido al pronto agotamiento de esta técnica, los fabricantes de antivirus han dotado a sus productos de métodos de búsqueda que no identifican específicamente al virus, sino a algunas de sus características generales y comportamiento.

Análisis Heurístico

Esta técnica se utiliza cuando no existe información suficiente para la detección de un virus nuevo; a través de ella se desensambla el código del virus para encontrar patrones sospechosos en los archivos (instrucciones como copiar, eliminar o sustituir código); además, se obtiene información de cada archivo (tamaño, fecha y hora de creación, entre otras) para que el antivirus la compare y verifique si se trata de un virus. El primer antivirus capaz de realizar análisis heurístico surge en 1989, pero, de manera casi paralela, aparecieron también los primeros virus con nuevas técnicas de ocultamiento.

A través de esta técnica pueden localizarse programas residentes en memoria, programas capaces de capturar aplicaciones en ejecución, código capaz de sobrescribir en memoria o modificar ejecutables, rutinas de cifrado u otras actividades propias de los virus. Por ello se recomienda disponer de un antivirus que combine el uso de "firmas de virus" con técnicas heurísticas.

Aunque las técnicas heurísticas representan un gran avance en la detección de virus desconocidos, presentan un serio inconveniente, ya que, al igual que otras técnicas de búsqueda, es muy alta la posibilidad de obtener "falsos positivos" o "falsos negativos".

[86] Término que puede ser traducido como "exploración".

Detecciones de Aplicaciones
Esta técnica permite detectar aplicaciones que se encuentran instaladas y actúan de manera oculta en equipos de cómputo, produciendo daños o realizando alguna acción maliciosa, tal como lo hacen los programas adware o spyware. La mayoría de los antivirus comerciales comienzan apenas a desarrollan esta técnica, pero se espera que pronto esté disponible como protección adicional al programa antivirus.

Detecciones Genéricas
Los antivirus pueden detectar programas maliciosos de forma genérica, es decir, encuentran nuevas variantes de virus que pertenecen a una familia determinada, la cual puede ser limpiada aunque el virus no haya sido descubierto aun o no se haya analizado su “firma”. Esta detección se indica como "Generic" en el nombre del virus, o mediante el sufijo "gen"; por ejemplo: W97M/Melissa.gen. Sin embargo, debido a las nuevas técnicas de ocultamiento y a la gran variedad de virus existentes, las técnicas de búsqueda deben afinarse casi diariamente para evitar que nuevos ataques tengan lugar.

4.2.2 Falsos Positivos y Falsos Negativos
Cuando un programa antivirus utiliza alguna técnica de búsqueda de virus, en ocasiones éstas no resultan del todo eficaces, produciendo errores conocidos como “falsos positivos” o “falsos negativos”. Un “falso positivo” se produce cuando el antivirus anuncia que un archivo está infectado, cuando en realidad está libre de virus. Caso contrario, un “falso negativo” sucede cuando el antivirus detecta que un archivo está limpio, cuando en realidad se encuentra infectado.

Ambos casos suelen presentarse de manera frecuente, aunque la situación menos deseada es que se presente un “falso negativo”, ya que el usuario estará confiado en que su programa antivirus realizó efectivamente su trabajo cuando en realidad su equipo (y demás recursos de cómputo) están en riesgo.

4.3 Métodos para determinar el Costo de un Ataque.
Cuando se intentan calcular los daños causados por un incidente de seguridad, existen posturas opuestas; por una parte, hay quien piensa que es imposible estimar ese valor debido a que no hay parámetros suficientes para hacerlo. Por ejemplo, cuando un virus infecta un equipo (o una red) se requiere, en el menor de los casos, ejecutar el programa antivirus; sin embargo, en casos más críticos, es necesario “formatear” el disco duro, para luego reinstalar el sistema operativo y las aplicaciones.

En este sentido, hay quienes consideran que no se han tenido pérdidas porque el problema se soluciona reinstalando programas y no se requiere desembolsar dinero por nuevas licencias de software; pero, quien sigue esta postura, no considera la pérdida de los archivos del usuario ni el tiempo invertido en restaurar los equipos afectados, lo que representa pérdida de productividad y de recursos económicos en la organización.

Por otro lado, algunas estimaciones mencionan, por ejemplo, que el virus Melissa provocó pérdidas por cerca de 80 millones de dólares (por lo cual el autor del virus fue sentenciado a 20 años de cárcel). Es aquí donde surge la pregunta, ¿cómo se obtuvo esa cifra? o ¿qué tan exacta es?.

Además, a pesar de que la cifra estimada pudiera parecer apegada a la realidad, existe la sospecha de que los auditores que ayudan a realizar estos cálculos modifican las cifras reales. Esta sospecha se fundamenta en que muchas compañías (principalmente instituciones financieras) no aportan datos verídicos sobre los ataques que han sufrido por miedo a la publicidad negativa. Considerando ambas posturas, ¿quién tiene la razón?, ¿puede calcularse el costo de los daños?, y si es así ¿cómo se realiza?.

4.3.1 Método de Encuestas.

A pesar de sus contraposiciones, ambas posturas coinciden que el mejor método para llegar a un estimado real es aplicar encuestas a las organizaciones (y a los encargados de la seguridad); las encuestas tienen como finalidad conocer al personal (y a la organización) que esta respondiendo el cuestionario. El estudio incluye preguntas específicas como: ¿quién se encargó de investigar el incidente?, ¿cuánto tiempo gastó en estas tareas?, ¿cuánta gente fue avisada del incidente?, ¿cuánto tiempo productivo perdió cada uno de los empleados?. Conocidos estos datos, resulta más sencillo calcular con certeza el costo de un incidente.

Compañías consultoras y organismos dedicados a la seguridad informática han aplicado el método de encuestas en diversos estudios, obteniendo resultados interesantes:

En promedio, las compañías de latinoamérica destinan a seguridad informática el 17% del presupuesto asignado Tecnología de Información (TI). En México, el 28% de los encuestados coinciden en que sus organizaciones perciben a la seguridad de la información como una prioridad; sin embargo, notan varios obstáculos para realizar un plan de seguridad efectivo, principalmente, la asignación presupuestal, la poca conciencia de los usuarios y la dificultad para mostrar el valor de la información[87].

En México existe además un aumento en la preocupación hacia el código malicioso, pero al mismo tiempo, estos problemas no son percibidos como una amenaza hacia la organización, sino como un tema exclusivamente tecnológico. El 40% de los encuestados reconocen que los virus y las fallas de hardware son las principales causas de interrupción de procesos productivos dentro en las organizaciones, de las cuales, el sector financiero, de telecomunicaciones y gubernamental son los mas afectados; por ello, sus principales preocupaciones son, en orden de importancia: protegerse de código malicioso y de la mala conducta de los usuarios, la seguridad física y el spam.

El estudio más reciente sobre seguridad informática en México[88] revela que, para los encargados de la seguridad, los ataques phishing, spyware y adware son la principal amenaza; pero, para el 58.3% de los administradores es más importante tomar medidas contra los ataques externos, mientras que el 32.8% señala que es más importante actuar contra atacantes internos. En cuanto a capacitación, el 30.0% de los administradores desea conocer sobre controles de acceso, el 22.8% sobre intrusos y el 18.3% sobre seguridad en Internet.

[87] Fuente: "Encuesta Global de Seguridad de la Información 2004", por Mancera Ernsts & Young. www.ey.com/mx

[88] "Estudio de Percepción sobre Seguridad en Informática 2005", por Joint Future Systems.
Fuente: "El Universal on Line", Lunes 26 de septiembre de 2005.

De hecho, el 90 % de las empresas no saben qué es spyware y aseguraron no tenerlo; pero el 100 por ciento tenían archivos de este tipo[89].

En cuanto a los usuarios, el 87.9% considera como principal amenaza a los virus, por ello, el 17.9% desea saber más sobre el tema, mientras que el 31.3% considera al antivirus como herramienta principal para proteger la información, y el 12.7% está interesado en saber sobre seguridad informática en general. Como posible solución a los problemas de seguridad, el 27.0% considera que se requiere mayor capacitación, el 25.7% cree que debe mejorar el manejo de contraseñas y un 24.0% cree que se necesitan políticas y controles de acceso.

El estudio demuestra además, que México sigue rezagado en seguridad informática, debido principalmente a la poca conciencia en los niveles directivos y también a que la seguridad no tiene la prioridad que se requiere al momento de asignar presupuestos. La ignorancia en este tema es evidente, ya que solo 3.8% de los entrevistados totales desea saber sobre políticas y procedimientos enfocados a la seguridad.

El estudio concluye con el planteamiento de varios retos, entre ellos, mayor difusión de la seguridad informática por parte de los proveedores de servicios de seguridad, a quienes, al mismo tiempo se les exige mayor honestidad al momento de dirigirse a sus clientes. Plantea además, el desarrollo de una conciencia de seguridad a todos los niveles y la creación de una legislación expedita y de normas de seguridad a nivel nacional, pero principalmente, contar con mayor capacitación y especialización, esencialmente, por parte de los participantes de esta industria.

Por otro lado, la encuesta[90] realizada por CSI[91] y FBI en Estados Unidos destaca que las pérdidas económicas causadas por ataques informáticos en empresas han bajado 61% con respecto al año anterior. Esta noticia pudiera parecer alentadora, sin embargo tiene un trasfondo muy grave, ya que ahora los ataques se enfocan a usuarios individuales, quienes están expuestos, principalmente, al robo de identidad.

A pesar de que estos resultados derivaron en algunas recomendaciones, existen problemas con el método de encuestas, ya que es difícil calcular la pérdida de productividad de los usuarios de un sistema averiado; pero el problema mayor es dar seguimiento al tiempo invertido a resolver incidentes de seguridad, ya que parte del tiempo de los encargados de seguridad se gasta administrando el antivirus o limpiando virus.

Por esto, los administradores son advertidos frecuentemente sobre la necesidad de tener un cuaderno a la mano y tomar nota de las acciones que realizan, la hora en la que las realizan y algunas notas adicionales, las cuales son la principal evidencia de que se realizaron las acciones y procedimientos correctos. Dichas notas sirven como respaldo para calcular el tiempo perdido y como referencias futuras en caso de que alguien más quiera trabajar en el mismo sistema; pero en la práctica nada de esto se hace.

[89] Fuente: Symantec, www.symantec.com
[90] "Computer Crime and Security Survey 2005"
[91] Computer Security Institute, dependiente del Federal Bureau of Investigations (FBI) de EUA.

4.3.2 El Modelo I-CAMP.

A mediados de los años 90's, las 10 universidades mas grandes de los Estados Unidos[92] iniciaron un proyecto para desarrollar un sistema para examinar el costo real de los incidentes de seguridad, dando como resultado el modelo conocido como *"Incident Cost Analysis Modeling Project"*[93]. Dicho modelo comprueba que las estimaciones de daños pueden producirse de manera exacta y con poco trabajo, pero deben realizarse con disciplina y diligencia por parte de quienes atienden incidentes de seguridad (punto donde se presentan mas deficiencias); por ello, el modelo propone que las políticas y procedimientos en el manejo de incidentes se implementen a nivel institucional y sea llevado a cabo de manera forzosa.

En 1999 se unieron más universidades a este proyecto buscando redefinir el modelo anterior, estudiar la frecuencia de los incidentes y desarrollar una clasificación de los mismos. Este esfuerzo derivó en "I-CAMP-II" a inicios del año 2000, el cual fue usado por primera vez en la Universidad de Washington (UW) después de una intrusión a un sistema de gran magnitud, formado por 18 equipos linux y cuyas pérdidas se calculan, en promedio, en US$1544 por host. Una de las razones por las que el incidente fue tan costoso es que los 18 sistemas tenían instalados programas que ayudaban al atacante a tener control total de los equipos; pero las pérdidas pudieron ser mayores porque el sistema de la UW fue solo parte de miles de sistemas alrededor del mundo que fueron comprometidos en el mismo periodo.

El modelo I-CAMP-II es directo y fácil de seguir, ya que considera el tiempo, los sueldos, horas extras y demás costos derivados de un incidente de seguridad. Así se deja claro que con preparación, políticas, procedimientos y disciplina durante el incidente, los resultados se logran de manera directa y con bastante precisión.

Para ilustrar este método, se plantea el ejemplo siguiente, que trata de obtener el costo del tiempo que un estudiante universitario pierde durante un incidente de seguridad en EUA. Para ello se asume que, en promedio, un estudiante toma 4 clases por semestre; cada clase requiere 12 horas de estudio por semana (3 horas de clase más 9 horas adicionales de estudio). Así, un estudiante debe estudiar 48 horas por semana o el equivalente a 192 horas por mes durante un semestre de 3.5 meses de duración, en promedio.

Considerando el costo de la colegiatura semestral por estudiante y dividiéndolo entre el total de horas por mes y la duración del semestre, se obtiene el pago por hora de estudio:

4 clases/semestre = 12 horas de estudio/semana = 48 horas/semana = 192 horas/mes
Duración del semestre = 3.5 meses
Colegiatura semestral = US$ 10,000.

Calculando: US$ 10,000 / (192 horas/mes * 3.5 meses/semestre) = US$14.88

[92] Grupo conocido como "Committee on Institutional Cooperation (CIC)" o "Big Ten".
[93] I-CAMP ó Proyecto para el Modelado del Análisis de Costos de Incidentes. http://www.cic.uiuc.edu.

Así, cuando un estudiante se ve envuelto en un incidente de seguridad, el costo del tiempo perdido es de US$14.88 por hora; en cambio, si el usuario es un profesor, el costo debe ser calculado considerando su sueldo. Sin embargo, cada universidad tiene diferentes costos, por lo que deben ser calcularlos considerando los mismos.

A pesar de que el método proporciona datos precisos y valiosos sobre incidentes de seguridad, no ha servido para cambiar la actitud de los directivos de las organizaciones, quienes asignan poco presupuesto y no apoyan en la implementación de políticas de seguridad. Por otro lado, las auditorias casi nunca toman en cuenta los costos por incidentes de seguridad, además de que los directivos casi nunca solicitan los datos sobre las pérdidas relacionadas con seguridad informática.

Es un hecho que un alto porcentaje de rectores de universidades, directivos de corporativos y funcionarios del gobierno no tienen idea del dinero perdido por incidentes de seguridad, lo que se traduce en una mala asignación de recursos, provocando que más ataques tengan lugar. El reto mayor de la comunidad dedicada a la seguridad informática es lograr el cálculo exacto de los incidentes, justificar los recursos asignados y evitar que ataques mayores sean realizados.

4.3.3 Daños estimados y sus cifras.

En nuestro país se han realizado diversos estudios tendientes a conocer los daños causados por ataques informáticos en las organizaciones, sin embargo, éstos se enfocan sólo a realizar estadísticas sobre el comportamiento de los usuarios o sus hábitos. No hay (por ahora) cifras estimadas sobre pérdidas económicas, por ello, este trabajo considera datos tomados de organismos nacionales e internacionales, que en el mejor de los casos, ofrecen cifras con 2 años de antigüedad, que sin embargo, plasman la realidad y dan una visión de la situación actual.

Por ejemplo, durante el año 2003, el valor del mercado de telecomunicaciones se ubicó alrededor de 1.1 billones de dólares, es decir, el equivalente al 3,1% del PIB[94] mundial; pero, si se añaden los ingresos de sectores vinculados a TI y comunicaciones, el conjunto representa del 10 al 15% del PIB mundial.

Por otro lado, se calcula que ataques de gusanos como w32.Blaster.worm, w32.Welchia.worm y w32/Sobig.F@mm provocaron pérdidas por el equivalente al 0.001% del PIB mundial, afectando principalmente servicios financieros, salud y energía. También en 2003, el gusano “w32/sobig” causó daños por el equivalente al 0.022% del PIB en EUA, y un año después, el gusano “w32/mydoom” provoco daños el 0.063% del PIB, es decir, las pérdidas se triplicaron en solo un año[95]. Por su parte, se calcula que el costo promedio anual del spam por empleado en Estados Unidos es de 1,934 dólares, ya que el empleado estadounidense promedio recibe casi 7 mil 500 mensajes de correo spam al año[96].

[94] PIB. Producto Interno Bruto. Se refiere al valor monetario de los bienes y servicios finales producidos por una economía en un período determinado.
[95] Con datos de e-mexico, Fondo Monetario Internacional, OCDE, US Departament of Treasure .
[96] Fuente: Nucleus Research www.nucleusresearch.com

Durante 2004 las organizaciones de todo el mundo gastaron alrededor del 0.015% del PIB mundial en protegerse de las nuevas amenazas de seguridad, como ataques web, spyware y phishing; ataques que se incrementaron 73%[97] con respecto al año anterior.

Por su parte, México ha participado desde 1994 con alrededor del 0.8%[98] del PIB Informático mundial[99], una de las tazas mas altas del mundo; aun así, nuestro país es de los que menos invierte en tecnología con el 0.5 % de su PIB nacional[100]. De hecho, los ataques informáticos durante 2004 provocaron el 35% de las pérdidas financieras en las empresas mexicanas; de ellos, el 50% fue provocado por virus o ataques internos; aunque también se presentaron otros incidentes, como robo de información, abuso de recursos informáticos, fraudes financieros, robo de dispositivos y accesos no autorizados.

Pero las pérdidas mayores fueron provocadas por ataques de virus, así como ataques de negación de servicio (que puede asociarse con virus o con intrusos)[101]. De ahí que los motivos de las empresas mexicanas para invertir en seguridad son: la protección de información (33%), los ataques de virus (23%), garantizar la continuidad de la operación (8%) y auditorias (7%)[102]. Por otro lado, el código malicioso (virus, gusanos y troyanos) se ubica como la preocupación número 1 (77%) en las empresas mexicanas, como se muestra en la (fig. 4.1):

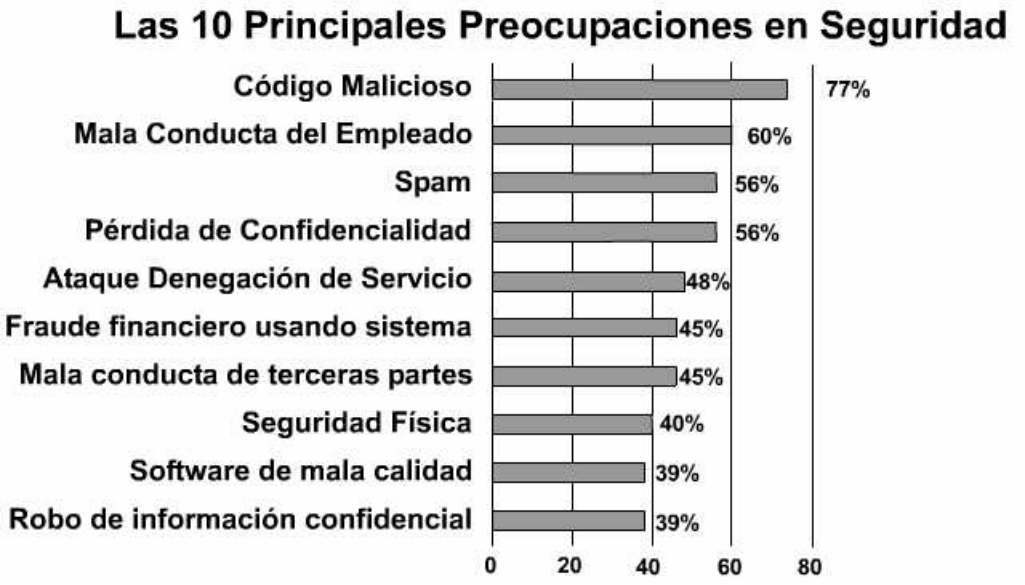


Fig 4.1. Las 10 principales preocupaciones en seguridad en México.

[97] Fuente: Elaboración propia con datos de e-mexico.
[98] Fuente: Indicadores sobre tecnologías de la Información INEGI, www.inegi.gob.mx
[99] Incluye productos y servicios de TI, cómputo y telecomunicaciones.
[100] Fuente: Con datos del Sistema de Cuentas Nacionales de México, INEGI. www.inegi.gob.mx y "El Economista" miércoles 12 de octubre de 2005, pp 28
[101] Fuente: McAfee. www.mcafee.com
[102] Fuente: VSAntivirus. www.vsantivirus.com/29-05-04.htm

Así, los principales obstáculos que observan las empresas para implementar un plan de seguridad eficaz son, en orden: la falta de conciencia por parte de los usuarios, restricciones presupuestales, falta de personal calificado, dificultad de probar el valor de la seguridad informática y los cambios tecnológicos constantes.[103]

Así concluye este capítulo, que intenta mostrar, además de las técnicas de detección de virus, el calculo más acertado sobre incidentes de seguridad, con el fin de concientizar a los usuarios de servicios de cómputo para que tomen conciencia sobre las consecuencias de un ataque; a los directivos de empresas para que asignen los recursos financieros, técnicos y humanos para prevenir ataques; y a autoridades gubernamentales para lograr una legislación en cuanto a seguridad informática se refiere.

El siguiente capítulo describe algunas técnicas, conocidas como “Buenas Prácticas” para limpiar y prevenir ataques por código malicioso, así como buenos hábitos de seguridad.

[103] Fuente: EY, www.ey.com

5

BUENAS PRÁCTICAS

Este capítulo brinda algunos consejos de seguridad para evitar ataques por código malicioso y ofrece además algunos procedimientos de limpieza de equipos infectados.

5.1 Introducción.

A pesar de la gran cantidad de noticias sobre código malicioso y sus efectos, son pocos los usuarios que conocen realmente su comportamiento o sus consecuencias. Por ello, es importante incrementar la cultura de la seguridad informática, lo que ayudaría, sin duda, a reducir riesgos de ataques y aumentaría la conciencia de los usuarios de servicios de cómputo. Pero, además de la capacitación, deben implementarse estrategias de seguridad acertadas y oportunas, las cuales se conocen como Buenas Prácticas (BP).

Las BP no son disposiciones legales, sino medidas prudentes y efectivas implementadas para proteger la información y garantizar los servicios de seguridad, de acuerdo a las necesidades específicas de una organización; las BP son también un método probado y validado por su aplicación en el campo de la seguridad; algunas BP parecen simples y obvias, pero son realmente esenciales.

5.2 Buenas Prácticas de uso común.

En este trabajo, se han mencionado ya los elementos principales del código malicioso, con el fin de conocerlo e implementar estrategias para combatirlo, las cuales pueden considerarse como un principio acertado de BP. Por ejemplo, para evitar la presencia de virus, debe procurarse la instalación de un antivirus en todos y cada uno de lo equipos de cómputo de la organización y complementar estas acciones con políticas de administración y uso del antivirus.

Es importante validar también que el antivirus se actualice periódicamente en todos los equipos para garantizar su efectividad; de hecho, muchos fabricantes antivirus permiten actualizar sus productos de manera automática, descargando desde Internet los archivos de firma de virus y demás parches en cuanto éstos son liberados. Se considera que un programa antivirus está actualizado cuando no tiene más de dos semanas a partir de la fecha de creación del archivo de firmas.

Se debe comprobar también que el antivirus incluya servicios adicionales como *soporte técnico*, que es de gran ayuda ante cualquier problema relacionado con virus o con el funcionamiento del antivirus; *resolución urgente de nuevos virus,* que en caso de verse afectado por algún virus de reciente creación, el proveedor analiza el virus, desarrolla su firma y la libera en el menor tiempo posible para evitar daños mayores; y el *servicio de alertas,* que notifica sobre el surgimiento de nuevos virus, este servicio se proporciona a través de listas de correo o por medio de un sitio en Internet con la descripción y características de los virus conocidos.

Como medida de adicional, el usuario debe generar una lista de lugares a donde pueda acudir en caso de emergencia, ya que no es recomendable esperar a que ocurra un siniestro para buscar ayuda. Dicha agenda debe incluir direcciones, teléfonos y correos electrónicos de las personas y organizaciones que puedan apoyar en caso de algún problema; si se cuenta con un antivirus comercial, deberán tenerse siempre a la mano los teléfonos de soporte técnico.

En cuanto al uso del antivirus, es importante validar que éste se encuentre siempre activo y efectuar una búsqueda de virus en todos y cada uno de los dispositivos de la red por lo menos una vez a la semana.

Por otro lado, es de especial cuidado el uso del correo electrónico, ya que es el medio que los virus utilizan en mayor medida para propagarse; por eso, cada mensaje recibido debe ser verificado antes de ser abierto, sobre todo porque ya no es necesario ejecutar el archivo adjunto para que el virus se active; en algunos sistemas basta con abrir el mensaje para que esto ocurra. Para evitar una infección, se recomienda no abrir los mensajes no solicitados o provenientes de destinatarios desconocidos, borrándolos inmediatamente. Actualmente, existen antivirus comerciales que se instalan en el servidor de correo electrónico, lo que permite verificar los correos entrantes y salientes automáticamente.

En las organizaciones, es importante tomar medidas en puntos de entrada a la red, así como en servidores de correo, de archivos y de aplicaciones; en cada uno de estos equipos se recomienda instalar software antivirus y realizar un seguimiento exhaustivo. También se debe tener cuidado con el uso de Internet, sobre todo al realizar descargas de programas desde sitios no seguros[104] ya que se pueden contener archivos infectados; por ello, se deben verificar dichos archivos antes de ser almacenados.

Gracias a Internet es posible (además de otros usos) conversar en tiempo real, intercambiar información y transferir archivos mediante grupos de noticias (news) y mensajeros instantáneos (chats); por ello, al utilizar estos servicios, es recomendable aceptar (con ciertas reservas) sólo los archivos provenientes de remitentes conocidos y de confianza, y rechazar archivos no solicitados, ya que actualmente, los virus aprovechan las vulnerabilidades de la mensajería instantánea para propagarse.

También se deben revisar las transferencias realizadas a través de redes P2P[105], ya que carece de monitoreo e incluye vulnerabilidades que aprovechan los virus para propagarse; además de que no siempre se conoce el origen de la información.

Otra vía de propagación de virus son los dispositivos removibles; por ello, antes de utilizarlos es importante analizarlos con el antivirus y cuando sean usados en otros equipos deberán protegerse contra escritura (en la medida de lo posible). En este punto, la conciencia de los usuarios juega un papel básico, de ahí la importancia de capacitarlos en el uso y manejo de dispositivos removibles como memorias flash y discos externos.

En cuanto a los disquetes, deben revisarse aunque sean nuevos y originales (grabados de fábrica), porque pueden contener virus por error del fabricante; y cuando se haya prestado alguno, debe ser revisado con el antivirus antes de usarlo nuevamente, ya que pudo haber sido infectado (intencional o accidentalmente).

[104] "Sitios no seguros" es aquel que no cuentan con información sobre su actividad, no es avalado por organismos de reconocido prestigio, o no cuentan con medidas de seguridad adecuadas.

[105] Se refiere a las redes "point to point" ("punto a punto"), en las que se pueden intercambiar archivos entre dos equipos remotos, los cuales comparten recursos para que otros usuarios tengan acceso a los mismos. El uso de estas redes se está generalizando día a día, lo cual es grave ya que no se lleva un registro de usuarios y carecen de monitoreo.

Una forma de evitar los virus de sector de arranque y de partición, es retirar el disquete de la unidad lectora al apagar o reiniciar el equipo; en caso de que esta acción sea olvidada por el usuario, conviene contar con un antivirus que compruebe la existencia de disquetes infectados; actualmente la mayoría de los antivirus comerciales realizan esta función.

Por otro lado, es importante contar con un disco de sistema libre de virus y protegido contra escritura, para acceder al disco duro en caso de que éste quede infectado, ya sea para respaldar la información contenida en él o para limpiarlo mediante alguna utilería.

Es bien sabido que los programas compresores permiten almacenar archivos y ocupar menos espacio en disco, aunque pueden también trabajar con archivos infectados; para minimizar riesgos, se recomienda guardar los archivos comprimidos en carpetas temporales antes de abrirlos y comprobar que el antivirus proteja el mayor número posible de formatos comprimidos.

Otra ventaja de los archivos comprimidos es que pueden protegerse mediante contraseña, lo que impide que personas ajenas tengan acceso al mismo; aunque, al mismo tiempo, se evita que el antivirus tenga acceso, y por lo tanto, en caso de contener virus, no puedan limpiarse. Se recomienda entonces, que cuando se busquen virus en un archivo comprimido, se quite la contraseña de protección, para luego ejecutar el programa antivirus y una vez explorado (y limpiado), se vuelva a proteger mediante contraseña.

Por su parte, los programas informáticos de uso común son más vulnerables a ataques de virus, por esta razón, los desarrolladores de software incluyen opciones de seguridad adicionales en sus productos, las cuales deben ser configuradas con una protección máxima y añadirlo en la política de protección del antivirus. Adicionalmente, existen actualizaciones que los fabricantes de software liberan para corregir o aumentar ciertas funcionalidades de sus productos, pero sobre todo, son actualizaciones que corrigen vulnerabilidades, por lo que es importante mantener actualizado todo el software instalado.

Por su parte, para minimizar el impacto de un virus se deben realizar copias periódicas y frecuentes de la información; así, la pérdida de datos puede ser superada mediante la restauración de la última copia de seguridad. Es recomendable tener respaldos de las áreas críticas del disco duro (sectores de arranque y de partición) y de los archivos ejecutables y de datos más importantes; para éstos últimos, conviene contar con doble respaldo, de preferencia, almacenados en lugares distintos, por si uno de ellos se daña.

También es importante verificar que existan rutinas de respaldo de información, así como planes de contingencia en caso de siniestro; ambas deben ser practicadas de manera periódica a manera de simulacro, además de estar documentadas para que se pueda dar seguimiento a estas acciones.

Otra forma de protegerse contra ataques, es informarse sobre hechos ocurridos en el sector de la seguridad informática, y aunque puede existir una gran cantidad de información en distintos medios, deben considerarse solo aquellas noticias difundidas por compañías antivirus, consultorías de seguridad, gobiernos o universidades.

Otro aspecto vital es no usar software ilegal; ya que, además de contener virus, viola derechos de autor y no permite disfrutar de los servicios adicionales que los fabricantes proporcionan junto con los productos originales. En este punto se recomienda implementar una política de instalación y manejo de software; por ejemplo, no usar software sin licencia o aquel que no sea necesario en la organización (como juegos o chats), vigilar el uso de los equipos y la instalación de software, capacitar a los usuarios sobre el manejo de estas políticas, así como autorizar el manejo y uso de software solo al personal que lo requiera.

Una acción adicional es exigir a los fabricantes de software, ISP[106] y editores de publicaciones, que se involucren en la lucha contra los virus, ya que en ella, se requiere la participación de todos los implicados en el sector informático: organizaciones públicas y privadas, usuarios finales, compañías antivirus, medios de comunicación, entre otros.

5.3 Limpieza de un equipo infectado.

Es factible que aún siguiendo las BP mencionadas, un virus pueda llegar a infectar los recursos de cómputo, ya sea por la ausencia de medidas de seguridad o por la explotación de vulnerabilidades por parte del virus; aun en estos casos, pueden tomarse algunas medidas generales con el fin de evitar que el virus se propague a otros equipos y al mismo tiempo, aislar y limpiar los recursos de cómputo ya infectados.

La primera acción a tomar cuando se sospecha de virus en ambientes de red es aislar los equipos infectados, es decir, ponerlos en “cuarentena” (misma acción que toman las autoridades sanitarias en caso de una epidemia). Para aislar los equipos infectados se debe desconectar físicamente el cable de red con el fin de que no tengan intercambio de información ni comunicación con otros equipos.

Posteriormente, debe “arrancarse en frío”, es decir, desde un disquete de sistema (libre de virus y protegido contra escritura) para eliminar virus residentes en memoria. Este procedimiento evita que el virus sea cargado en memoria y sea más fácil su detección y eliminación, de acuerdo al procedimiento adecuado para cada tipo de virus. En el Capítulo 3 se explicó ampliamente la estructura y funcionamiento de los discos duros, así como de los virus de partición y de arranque. En esta sección se pretende describir algunos procedimientos generales para limpiar virus de este tipo.

5.3.1 Limpieza de Virus en Sector de Partición.

Para iniciar el procedimiento de limpieza se debe contar con un disquete de arranque generado en una computadora libre de virus; es importante verificar que el equipo inicie desde el la unidad de disquete y encender el equipo con el disquete de arranque dentro, esto dará acceso al disco en modo línea de comando de MS-DOS.

Para efectuar el procedimiento debe considerarse que en algunos sistemas operativos de Windows, el comando FDISK regenera automáticamente el MBR del disco duro sin pedir confirmación. Sin embargo, si el disco fue particionado por medio de alguna utilería (como “Disk Manager” o “EZ”), al aplicar este procedimiento se corre el riesgo de dejar inaccesible el disco, y por lo tanto, perder acceso a la información almacenada.

[106] ISP: *Internet Service Provider*. Proveedor de servicio de Internet.

Es decir, para que este procedimiento funcione, se requiere contar con partición FAT y disco duro particionado mediante FDISK. En cambio, si un virus infecta un disco duro con sistema de archivos NTFS[107] se debe usar la "Consola de Recuperación de Windows" para acceder a estas particiones. Este sistema de archivos es propietario de Windows NT (que incluye las versiones 2000, XP y 2003), la cual implementa seguridad a nivel de archivo, es decir, cada archivo (o directorio) posee su lista de control de acceso que determina a los usuarios que tienen derechos sobre él, especificando claramente los permisos de cada uno.

La forma más simple de iniciar la Consola de Recuperación es mediante un disquete de inicio, ó utilizar el CD de instalación de Windows y ejecutar el comando:

../i386/winnt.exe (desde DOS), o
../i386/winnt32.exe (desde Windows) para restaurar la partición.

5.3.2 Limpieza de Virus en Sector de Arranque.

Para limpiar el sector de arranque de un disco duro infectado se debe aplicar el procedimiento correspondiente de acuerdo al sistema operativo; en el caso de Windows con sistema FAT se debe generar un disco de arranque en un equipo libre de virus y con el mismo S.O. del equipo infectado, para luego iniciar éste con el disquete de sistema; esto abrirá una sesión en modo línea de comando, donde se deberá ejecutar el comando ***a:\> sys c:***, lo que restaurará el sector de arranque.

Para Windows con sistema NTFS, el equipo deberá iniciarse desde CD de arranque de Windows y elegir la opción "recuperar" para entrar a la "Consola de Recuperación", cuando ésta se inicie, se deberá ejecutar el comando ***fixmbr*** para reparar el MBR; para realizar este procedimiento es importante contar con la contraseña de administrador del equipo, de lo contrario no se tendrá acceso al equipo y no se completará el procedimiento.

Además de los procedimientos anteriores, existen algunas herramientas comerciales que podrán ayudar a eliminar este tipo de virus, como la ofrecida por la compañía McAfee, la cual se puede descargar de manera gratuita desde:

http://download.nai.com/products/mcafee-avert/em_dats/emscan.zip

Al acceder al sitio, se tendrá acceso a un archivo comprimido en formato ZIP, que deberá descargarse en un equipo libre de virus; luego se deberán copiar los archivos en un disquete e iniciar la computadora infectada con un disquete de inicio limpio. Cuando aparezca el símbolo de sistema (**a:**) deberá teclearse:

- Para particiones FAT: **bootscan c: /boot /clean /nomem**
- Para particiones NTFS: **bootscan c: /boot /clean**

Al final, se debe retirar el disquete, reiniciar el equipo y mantenerlo en observación por un periodo razonable; si no hay ninguna anomalía, podrá conectarse nuevamente a la red.

[107] NTFS: New Technology File System ó Sistema de Archivos de Nueva Tecnología.

5.3.3 Limpieza de otros tipos de Virus.

Debido a que los virus informáticos son cada vez más sofisticados, es difícil sospechar su presencia “a simple vista”, sin embargo, algunos síntomas generales en una computadora infectada pueden ser, entre otros: procesamiento más lento, retraso al cargar los programas, accesos no solicitados a disqueteras o al disco duro, disminución de la memoria RAM y del espacio disponible en el disco duro, o aparición de programas desconocidos residentes en memoria.

Ante estos síntomas es recomendable realizar una exploración en busca de virus; pero, como ya se mencionó, algunos virus pueden inhibir la acción del antivirus y hacer creer que éste se encuentra activo. Para evitar estas acciones, existe un procedimiento que permite buscar virus en todos y cada uno de los archivos alojados en el disco duro.

Este procedimiento consiste en descargar el archivo llamado “SuperDat”[108], de acuerdo al procedimiento mencionado a continuación:

1. Crear una carpeta temporal en la unidad c:\ y llamarla, por ejemplo, *antivirus.*

2. Ir a http://www.mcafee.com/apps/downloads/security_updates/dat.asp?region=us&segment=enterprise, donde se encuentra una lista de utilerías, entre ellas, el archivo SuperDat con el nombre “Superdat File (engine+dat) ó “sdatxxxx.exe”[109].

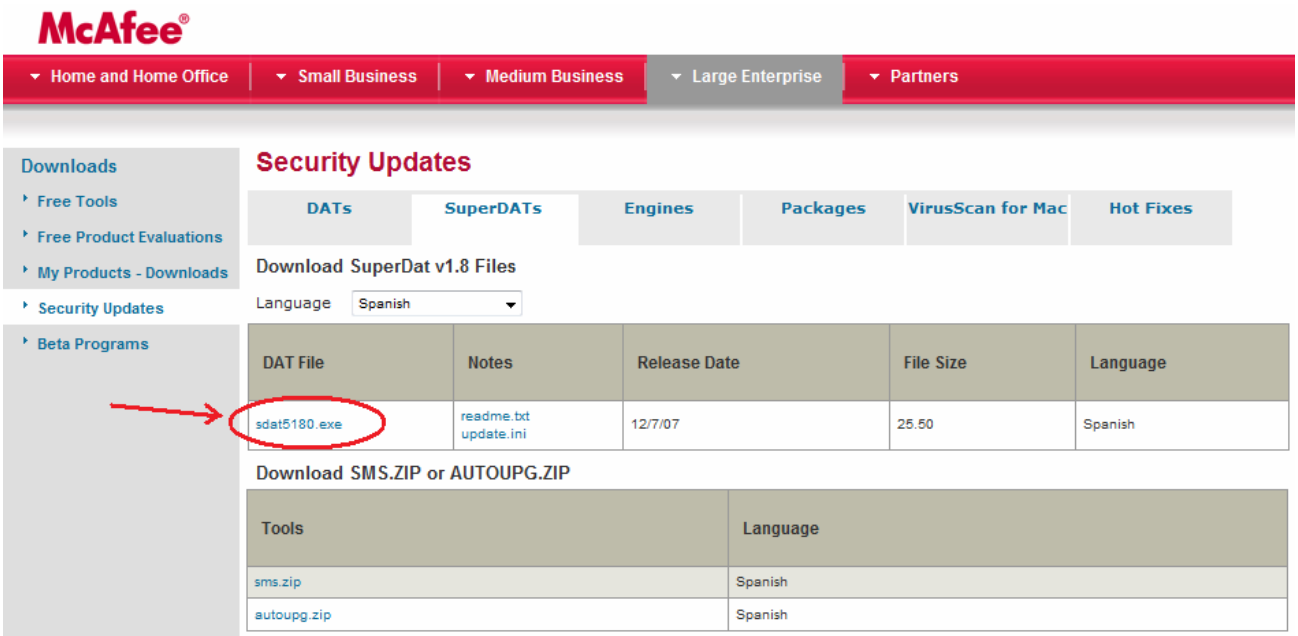


Fig 5.1. Descarga del archivo DAT .

[108] Archivo de firmas que utiliza la marca McAfee para actualizar semanalmente su antivirus. www.mcafee.com
[109] Las x corresponden a un número consecutivo correspondiente al número de la versión del archivo, por ejemplo, sdat5210.exe

3. Descargar el archivo en la carpeta *antivirus;* concluida la descarga, reiniciar el equipo en modo “símbolo de sistema” ó “a prueba de fallos”. Esto se logra iniciando el equipo e intermitentemente oprimir la tecla <F8> hasta que aparezca el menú y se elija alguna de las opciones mencionadas. Con este procedimiento, el equipo es iniciado “en frio”, evitando que el virus se cargue en memoria y que no pueda ocultarse.

4. Iniciado el sistema, debe ejecutarse el comando ***sdatxxxx.exe*** con el parámetro ***/e*** (que significa expandir) para descomprimir en la carpeta *antivirus* los archivos que contiene el archivo ejecutable, como se muestra: `C:\antivirus>sdat4510.exe /e`

5. Descomprimidos los archivos, debe ejecutarse el comando ***scanpm /adl /clean /all,*** que iniciará una búsqueda de virus en todos y cada uno de los archivos alojados en el disco duro; el comando utiliza la siguiente interfaz, donde se indica la versión de archivo DAT utilizada, su fecha de creación y el archivo explorado:

```
C:\antivirus>scanpm /adl /clean /all
McAfee VirusScan for DOS/PM v4.40.0
Copyright (c) 1992-2004 Networks Associates Technology Inc. All rights reserved.

(408) 988-3832  LICENSED COPY - Sep 23 2004

Scan engine v4.4.00 for DOS/PM.
Virus data file v4510 created Jun 09 2005
Scanning for 130342 viruses, trojans and variants.

Checking memory for viruses ... is OK.


Scanning C: []
Scanning C:\*.*
C:\APACHE~1\ERROR  -
```

El procedimiento detectará y limpiará archivos infectados automáticamente; sin embargo, es importante que después de limpiar el equipo se instalen los parches correspondientes tanto de sistema operativo como de los programas instalados.

Adicionalmente, si el equipo infectado cuenta con S.O. Windows ME o Windows XP se debe quitar la “Opción de Restaurar Sistema”, la cual permite efectuar respaldos de los archivos de sistema, pero, si éstos están infectados, el respaldo también se guarda infectado en un área restringida; el hecho de quitar esta opción permite tener acceso a esa área de sistema y limpiar los archivos.

5.4 Herramientas de Prevención.

Para facilitar la prevención y erradicación de código malicioso, además de las BP, diversas compañías se han dado a la tarea de desarrollar herramientas prácticas que permiten que incluso un usuario inexperto pueda utilizarlas.

5.4.1 EICAR

Cuando un usuario instala un antivirus, no existen procedimientos que permitan verificar que éste funcione correctamente; por ello, EICAR[110] desarrolló una utilería que permite comprobar de manera concreta si el antivirus detecta y detiene una posible infección.

[110] European Institute for Computer Anti-Virus Research o Instituto Europeo para Investigación Antivirus.

Esta herramienta se conoce como “Virus de Prueba EICAR” y funciona con todos los productos de los fabricantes de antivirus pertenecientes a dicha asociación. A través de él se pueden validar con pruebas no dañinas y en un ambiente real, las políticas antivirus implementadas en la organización; sirve también para medir la efectividad del antivirus.

Este virus de prueba consiste en un archivo de 68 caracteres imprimibles en código ASCII y que puede ser creado con un editor de texto de acuerdo a la siguiente cadena:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

De manera opcional, la cadena puede ser rellenada con espacios en blanco sin exceder los 128 caracteres de longitud; los únicos caracteres permitidos son el carácter de espacio, tab, LF, CR y CTRL-Z. Es importante señalar que tercer caracter de la cadena es la letra mayúscula “O” y no un 0 (cero) y que Eicar solo funciona en archivos ubicados al mismo nivel en la estructura de directorios.

Para crear el “virus de prueba EICAR” se abre un editor de texto y se escribe (o copia) la cadena de caracteres mencionada, luego se guarda el archivo con el nombre *eicar.com* y utilizarse, por ejemplo, para ser enviado como archivo adjunto de correo electrónico y probar el antivirus del servidor de correo, compartirse a través de recursos en red y probar el antivirus de servidores y estaciones de trabajo o añadirlo a un archivo comprimido.

En cualquiera de los casos, el antivirus debe detectar y producir una alerta, ya que el archivo no puede ser borrado; por ello, algunos antivirus lo colocan en la carpeta de cuarentena y otros lo renombran como *eicar.com.vir p*ara indicar que el archivo esta infectado. Cualquier caso representa el trato que recibiría un virus real.

5.4.2 Ad-Aware

Como se mencionó en el Capítulo 3, adaware son programas que se instalan y actúan de manera oculta para mostrar publicidad no solicitada, por lo que el usuario no percibe su presencia. En el mercado existen diversas herramientas que ayudan a combatirlo, pero una de las más populares es “Ad-aware”, desarrollado por la compañía “Lavasoft”.

Existe una versión gratuita instalable en cualquier versión de Windows y compatible con los antivirus comerciales, lo que permite tener ambos productos en el mismo equipo y complementar la protección que ofrece cada uno. “Ad-aware” realiza una búsqueda en carpetas, archivos (de datos, configuración y sistema) y en el registro de Windows, indicando la unidad que se está explorando, el archivo, su ruta, un contador de archivos explorados y la cantidad de programas maliciosos encontrados (Fig. 5.2).

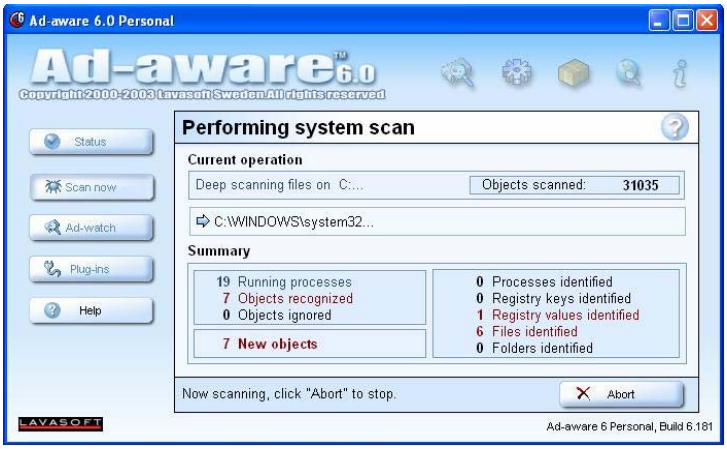


Fig 5.2 Exploración con Ad-Aware

Terminada la exploración, aparecerá un reporte con el nombre, tipo y ruta del elemento malicioso encontrado; el programa ofrece la opción de eliminar el contenido encontrado o colocarlo en una carpeta en cuarentena. Así, todo el maleware detectado será deshabilitado del equipo (Fig. 5.3). Sin embargo, para que el proceso de búsqueda sea mas efectivo, es necesario descargar las actualizaciones de "Ad-Aware" desde Internet, con el fin de tener instaladas las "firmas" de nuevos ataques.

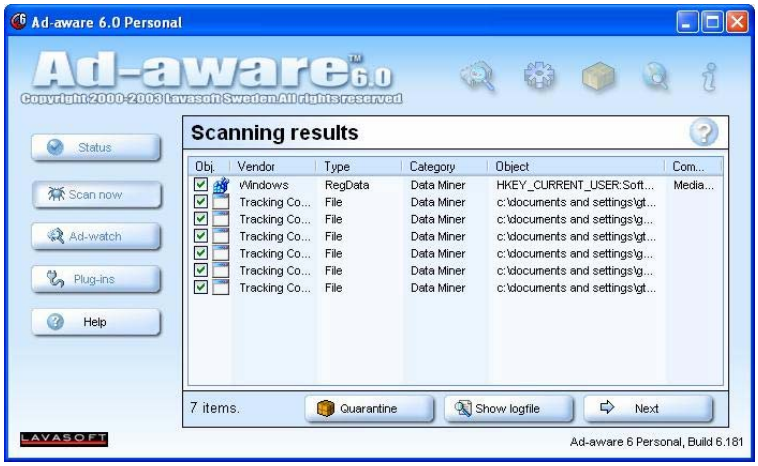


Fig 5.3 Reporte de Exploración con Ad-Aware

5.4.3 Anti - Spam

Para no ser victima de un ataque se debe evitar abrir, reenviar o contestar correo spam, ya que algunos de estos mensajes ofrecen borrar de la lista de envío a quien conteste el mensaje y escriba como titulo del mismo "borrar" o "eliminar". Muchos mensajes spam son enviados "al tanteo" por parte del remitente, es decir, tratando de adivinar alguna dirección de correo valida; el hecho de contestar estos correos le da la oportunidad al atacante de validar que esa cuenta de correo existe y por lo tanto, puede ser atacada.

Los mensajes phising y spam pueden contener software que grabe información sobre la actividad del equipo atacado o dejar "backdoors" abiertos para permitir al atacante entrar al equipo y tomar control del mismo.

Cuando se envíen copias de un mensaje a varios destinatarios, se debe procurar escribir las direcciones de los mismos en el campo *"cco" (con copia oculta)*, ya que si dichas direcciones se incluyen en el campo *"para"* quedan expuestas a ser atacadas con mensajes spam. También se debe tener cuidado al inscribir una cuenta de correo electrónico en grupos de noticias o foros en Internet, ya que muchos atacantes toman las direcciones de correo de estos sitios; además, al usar este tipo de servicios no se debe de proporcionar la cuenta de correo principal, sino una dirección alternativa (cada usuario debe tener una o dos adicionales). Por otro lado, no deben efectuarse compras desde sitios no solicitados o desconocidos.

5.4.4 Anti-Phishing

Como ya se mencionó en capítulos anteriores, *Phishing* es un ataque cuyo objetivo es robar contraseñas e información confidencial a través de correos apócrifos, que redireccionan al usuario atacado hacia páginas de Internet falsas, donde se le pide "confirmar" sus datos confidenciales.

De acuerdo con cifras de *Anti-Phishing Working Group*, los atacantes pueden convencer a cerca del 5 % de los usuarios atacados a proporcionar sus datos. Como forma de prevenir este ataque, se recomienda nunca responder correos electrónicos donde se solicite información personal.

De hecho, la mayoría de los mensajes phishing incluyen en el título del mensaje "urgente – tus datos pueden ser robados" con el fin de provocar una reacción inmediata. Cabe mencionar que las compañías de reconocido prestigio no solicitan a sus clientes o usuarios información confidencial a través de correo electrónico.

Otra medida de prevención es teclear la dirección completa del banco o institución que se desee visitar, es decir, nunca usar ligas o la barra de acceso. Además, se debe verificar que la página visitada sea segura, para esto, antes de entrar a la página debe verificar que la dirección URL de la página inicie con https[111] en lugar de http; así también se puede verificar la existencia de un icono en forma de candado en la barra de estado y verificar la validez del certificado digital.

De esta manera concluye este capítulo, que describe las Buenas Prácticas más comunes para los ataques conocidos, sin embargo, éstas pueden cambiar de acuerdo a la forma en que evoluciones también lo nuevos ataques. El siguiente capítulo brinda un panorama precisamente de la evolución del código malicioso.

[111] En https, la letra "s" significa que el protocolo HTTP tiene implementada seguridad a través e algún protocolo.

6

TENDENCIAS FUTURAS

Este capítulo muestra un panorama sobre el código malicioso y su evolución a través del tiempo, proceso que va de la mano con los avances tecnológicos.

6.1 Introducción.

Observando el comportamiento de los virus en la última década, se puede notar que han aumentado en número y en peligrosidad de manera constante; cada año, el número de virus descubiertos aumenta, además de que aparecen métodos de infección más devastadores; al mismo tiempo, surgen más variantes, provocando que las familias de virus sean cada vez más numerosas.

Por muchos años, los virus de macro habían sido el problema más grande que enfrentaban las organizaciones, debido a la facilidad para crearlos y su capacidad para propagarse a través de recursos de red o de archivos adjuntos de correo electrónico. Sin embargo, con la aparición de virus con nuevas técnicas de infección y propagación (como *Melissa*), se dieron muchos cambios tanto en la creación como en el combate de los virus.

Hoy en día, los gusanos y el correo masivos representan más del 49% de los virus reportados en campo, adicionalmente, el 12% de los virus afectan sistemas operativos de 32 bits y no son de macro; de hecho, menos del 30% de los virus reportados son de macro[112]; estos datos reflejan que la realidad de los virus ha cambiado.

Lo que es un hecho, es que cada día se aprecia mayor dependencia a la tecnología en las actividades cotidianas, convirtiendo a las TI y las comunicaciones en herramientas casi imprescindibles; por ejemplo, las nuevas tecnologías de comunicación (que abarca diferentes medios e incluye diversos dispositivos electrónicos) podrían llevar en un futuro próximo a la creación de una nueva generación de virus que interfieran con cualquiera de estos dispositivos, como teléfonos celulares, agendas electrónicas, e incluso, equipos de navegación en autos o aviones, entre muchos otros.

6.2 La tendencia de los virus.

La situación descrita, que hace algunos años podía parecer irreal, se ha convertido en una realidad, ya que diversas compañías antivirus detectaron recientemente código malicioso en dispositivos móviles distintos a las computadoras.

Un caso lo representa el virus *"Symbos_Cabir.A"*, que infecta el sistema para teléfonos celulares "*Symbian".* Otro caso conocido es *"W64_Shruggle"*, virus que afecta sistemas con Windows de 64 bits, y que es considerado una prueba para demostrar las vulnerabilidades de dicho sistema. Ambos virus atacan también dispositivos PDA[113] equipados con Windows CE.

Por otro lado, en mayo de 2005, se detectó un nuevo modelo de virus para sistemas que corren en Windows de 64 bits llamado "*W64_Rugrat.A*", el cual despertó grandes expectativas sobre la posibilidad de que sus creadores estuvieran experimentando sobre estos sistemas operativos para ambientes empresariales.

[112] Fuente: McAfee. www.mcafee.com
[113] PDA: Del inglés *Personal Digital Assistant* ó Ayudante personal digital; se refiere a Agendas Electrónicas.

Esta preocupación se deriva en el hecho de que *Windows 64* es un sistema operativo que soporta datos en paquetes de 64 bits, por lo tanto, duplica la capacidad de procesamiento de datos y hace más eficiente la lectura y escritura en discos y memoria, entre otras ventajas. Los primeros análisis de "Rugrat.A" llevaron al descubrimiento de que estaba programado con las mismas técnicas de otro virus de 32 bits llamado "Shrug.A" (detectado en 2003), y que estaba habilitado para infectar archivos sin ser detectado por el sistema.

Por su parte, *"W64_Shruggle.A"* es una versión muy similar a *"Rugrat"*, pero muestra una diferencia muy importante, ya que éste último fue diseñado para infectar sistemas de 64 bits que utilizan el procesador IA64[114]; de hecho, *"Shruggle"* hace lo mismo, pero sólo en los procesadores AMD64[115], lo que fortalece la idea de que el virus no fue creado con el propósito de desencadenar una epidemia informática, sino para demostrar la vulnerabilidad de un sistema como Windows de 64 bits.

Después de ejecutarse, el virus busca archivos a infectar en la misma carpeta (y subcarpetas) donde se ha copiado el archivo infectado; luego, busca todos los archivos de 64 bits que encuentra (sólo en sistemas con procesadores AMD64) y los hace pasar por ciertos criterios de selección. Por ejemplo, a algunos les agrega su propio código en la parte final, y modifica esta sección para hacerla ejecutable; junto al código del virus se agregan también datos basura, que son utilizados para ocultarse.

Los archivos infectados crecen en aproximadamente 1,318 bytes. Este virus no infecta archivos de 32 bits y tampoco se ejecuta en procesadores sin el software para soportar programas de AMD64; sin embargo, los archivos infectados poseen el texto de firma: "Shrug - roy g biv".

Fig 6.1. Interfaz del virus Commwarrior.

Otra seria amenaza es "Commwarrior", el primer virus que se transmite a teléfonos celulares mediante mensajes multimedia o de texto[116] enviados a los miembros de la lista de contactos del equipo atacado. Por ahora, el virus está limitado a teléfonos de la *Serie 60* de *Nokia* que utilizan "Symbian OS" [117], aunque se sospecha que el virus también se puede propagarse con la tecnología inalámbrica Bluetooth, como se muestra (Fig 6.1).

El virus afecta archivos *.SIS* y se hace pasar por aplicaciones validas como juegos, simuladores o pornografía; después se replica usando tecnología MMS[118], la cual permite crear, enviar, y recibir mensajes de texto, e incluso imágenes, audio y video.

[114] Intel Titanium, el primer microprocesador para 64 bits en el mercado.
[115] Versión de microprocesador a 64 bits de la compañía Advanced Micro Devices.
[116] Fuente: "El Universal on Line". Jueves 10 de marzo de 2005. Primera sección, página 14 y www.mcafee.com
[117] Según datos de la empresa de seguridad informática F-Secure
[118] MMS: Multimedia Messaging Service, Servicio de Mensajería Multimedia

Fig 6.2. Instalación .SIS

Un mensaje MMS puede ser enviado de teléfono a teléfono o directamente a una cuenta de correo electrónico, una vez que se encuentra en la bandeja de entrada del dispositivo infectado, el usuario puede verlo para aprobar la instalación del archivo .SIS. Al instalarlo, el virus se ejecuta de manera automática cada vez que el dispositivo se inicia; posteriormente, se despliega un mensaje en pantalla que solicita instalar la aplicación (que lleva oculto al virus). El texto del mensaje puede ser muy variado, pero el efecto del virus es el mismo.

A través de diversos análisis se ha observado que el código del virus contiene el siguiente mensaje, probablemente escrito por su autor:

CommWarrior v1.0 (c) 2005 by e10d0r
CommWarrior is freeware product. You may freely distribute it in it's original unmodified form.
OTMOP03KAM HET!

Las consecuencias inmediatas de la infección son, por ejemplo, el rápido agotamiento de la batería. Además, el virus tratará de enviarse a todos los contactos almacenados en la libreta de direcciones, provocando el envío indiscriminado de mensajes, y por tanto, una factura con cargos exorbitantes por el servicio de envío de mensajes.

Por otro lado, un fenómeno interesante que se ha observado durante los últimos años, es el decremento en el número de correos electrónicos que contienen código malicioso. Por ejemplo, durante 2005 se observó que en promedio, 1 de cada 36.15 correos electrónicos (2.8%) contenía código malicioso, cifra que contrasta con la observada en 2004, donde 1 de cada 16.39 (6.1%) correos enviados contenía código malicioso[119].

Esta tendencia indica que el correo electrónico “tradicional” quedará de lado, y su lugar será ocupado por los dispositivos móviles como el blanco preferido para ser atacado; lo que indica también que los atacantes buscan nuevas formas para hacer daño.

6.3 Las nuevas formas de SPAM.

Hasta ahora, el spam es originado por compañías cuyo negocio es hacer publicidad a través de correo electrónico masivo. Al día de hoy, los dispositivos móviles habían estado al margen de este tipo de mensajes, sin embargo, algunas compañías trasnacionales (como Procter & Gamble y Mc Donald’s) han comenzado a enviar mensajes spam a los celulares de sus clientes (quienes voluntariamente proporcionan sus datos para este y otros servicios[120]) en los Estados Unidos.

Desafortunadamente, este no es el único caso, ya que en Europa, la ITU[121] calcula que cerca del 80 % de los usuarios de teléfonos celulares ha recibido correo spam.

[119] Fuente: IBM Global Business Security Index Report in 2005 and Outlook for 2006.
[120] Fuente: “El Economista” Sección IT, lunes 1 de Agosto de 2005, pp4. “El escurridizo spam”, por: Roberto Gaona.
[121] International Communications Union ó Union Internacional de Comunicaciones.

En México, compañías que proporcionan servicios de mensajería a través de teléfonos celulares (como envío de noticias generales o entretenimiento) brindan el servicio para el que fueron contratados, pero además, envían mensajes spam a sus usuarios, promocionando diversos productos y servicios.

El éxito del spam radica en que es publicidad mucho más barata que la que se puede realizar por cualquier otro medio, como prensa escrita, radio o televisión; otra ventaja es que llega al potencial cliente de manera directa.

La tendencia para los próximos años es que el spam (y también otro tipo de código malicioso) llegue a afectar teléfono celulares, PDA's y otros dispositivos inalámbricos. Sin embargo, no se ha generalizado su propagación porque este tipo de código no puede reproducirse por sí mismo en estos dispositivos (hasta ahora); aunque la tendencia a usar dispositivos móviles provocará que tenga mayor atención en un futuro muy próximo.

6.4. Tendencias de los ataques Phishing.

Phishing fue la amenaza más frecuente durante 2005 (1 de cada 304 correos incluía código phishing); sin embargo, este porcentaje es sensiblemente menor al observado durante 2004, donde 1 de cada 943 correos contenía spam[122].

Se cree que este decremento se debe a que el correo electrónico está quedando de lado como medio de propagación de código malicioso, ya que nuevos dispositivos móviles se harán más populares en este sentido. Además, los atacantes han incrementado su capacidad, tanto tecnológica como intelectual, lo que les permite hacer uso de nuevas técnicas de envío de correo masivo, y de esta forma, efectuar ataques a objetivos cada vez más definidos y potencialmente más dañinos.

Una nueva variante de phishing conocida como "Spear Phishing" [123] amenaza con ir en aumento en los próximos años. Mediante este ataque los criminales saturan la red de las organizaciones con mensajes spam que parecen ser originados desde dentro de la empresa, generalmente el departamento de informática o de recursos humanos. El atacante, basado en "ingeniería social"[124], ofrece una pequeña recompensa a los usuarios que proporcionen información sobre la organización, su infraestructura, o sus empleados.
De esta manera, los usuarios creen que el correo es legítimo y contestan ingenuamente la solicitud; con esta información, el atacante puede tener acceso a áreas restringidas de la red corporativa y obtener información o datos sensibles.

Estos ataques podrían ser mejorados por parte de los atacantes en un futuro próximo; aunque claramente se observa que el eslabón más débil de la seguridad seguirán siendo los usuarios. La capacitación y la concientización serán definitivas en el combate a estos problemas.

[122] Fuente: IBM Global Business Security Index Report in 2005 and Outlook for 2006.
[123] Término que puede traducirse como "pescar con arpón"; implica una pesca dirigida a un objetivo concreto.
[124] Ataque basado en engañar a las personas, con el fin de que proporcionen (de manera inadvertida) información sobre su actividad, su propia persona o su organización.

6.5 Perspectivas[125].

Durante el 2005 se observó un fenómeno que no se había visto antes, que es la mezcla compleja de distintos tipos de código malicioso. Por ejemplo, el gusano “Mytob” se basa en el gusano “Mydoom” y además agrega otras funcionalidades, provocando la aparición de otras variantes del “Mytob” mucho más peligrosas.

En ese mismo año, dos de cada tres ataques de correo electrónico fueron interceptados cada semana, los cuales fueron provocados por motivos financieros, comerciales, políticos o sociales; y casi siempre fueron dirigidos a oficinas gubernamentales, militares u otras organizaciones dedicadas particularmente a actividades aeroespaciales, petroleras, de impartición de justicia y de derechos humanos. Lo anterior indica que el esquema y los motivos para iniciar un ataque han cambiado, ya que anteriormente se atacaban preferentemente instituciones financieras, académicas o comerciales.

Por otro lado, los desarrolladores de software enfocan sus esfuerzos en hacer más seguros sus productos, lo que puede ayudar a disminuir el número y la peligrosidad de los ataques. Sin embargo, las compañías se enfrentan a diversos riesgos como, falta de capacitación de los usuarios, recursos globales, despido de empleados y fusiones con otras compañías.

Todos estos fenómenos incrementan la cantidad y potencialidad de los ataques internos, aunque se prevé que en el futuro, los ataques estén dirigidos al usuario final y que los criminales enfocarán sus esfuerzos en engañar a los usuarios para que éstos ayuden a efectuar el ataque, en lugar de perder tiempo en descubrir una vulnerabilidad.

En la actualidad, la situación se agrava debido a que los atacantes toman ventaja de la poca cooperación internacional relacionada con delitos (principalmente informáticos), lo que ha hecho más difícil rastrear a los criminales. Ellos tratan de “hacer puente” entre países desarrollados (donde se inicia el ataque) y economías emergentes (donde se produce el ataque), como países del este de Europa, Asia, y América Latina, donde no existen legislaciones contra delitos informáticos.

De esta manera concluye este capítulo donde se describió un panorama de las tendencias de la seguridad y del código malicioso. En la siguiente sección de este trabajo se enuncian las conclusiones finales del mismo.

[125] Fuente: IBM Global Business Security Index Report in 2005 and Outlook for 2006.

CONCLUSIONES

La Seguridad surgió a partir de la necesidad de proteger los conocimientos generados por un grupo o tribu y ha evolucionado paralelamente con la tecnología; sin embargo, con el surgimiento de las computadoras, ha tomado una importancia relevante.

Cuando comenzaron a utilizarse las computadoras como medio de producción, sólo unas cuantas organizaciones tenían los recursos para contar con uno de estos equipos; las nuevas formas de producción y el avance tecnológico influyeron para que más empresas realizaran sus procesos a través de computadoras. Con el surgimiento de Internet, las organizaciones y las personas se preocuparon por integrarse a esa red, dando origen a muchos y muy variados problemas de seguridad informática.

Actualmente, muchas instituciones cuentan con una conexión a Internet, pero son pocas las que se han preocupado por asegurar su información y sus procesos. El hecho de no contar con un área de seguridad en cómputo dentro del organigrama provoca que el administrador de la red y el personal asignado al área de sistemas, además de sus tareas diarias, deba lidiar con los problemas de seguridad, y al ocupar demasiado tiempo resolviendo problemas, provocan que los ataques sean exitosos.

A través de diversos estudios, se ha observado que los principales obstáculos que tienen las empresas para implementar un plan de seguridad eficaz son: la falta de conciencia de los usuarios para utilizar los servicios de cómputo de manera adecuada, la falta de personal calificado en el área de seguridad, pero sobre todo, los cambios tecnológicos constantes y las restricciones presupuestales. En este último rubro cabe hacer mención que cuando existe un nuevo proyecto de sistemas, la organización destina recursos (tiempo y dinero) muy limitados, por lo que la prioridad se da a que el sistema funcione lo antes posible dejando de lado la seguridad.

Otro hecho importante que afecta a la implementación de mecanismos y políticas de seguridad es el calcular el valor de la información; puede decirse que un alto porcentaje de rectores de universidades, directivos de empresas y funcionarios del gobierno no tienen idea clara del dinero perdido por incidentes de seguridad, lo que se traduce en una mala asignación de recursos, provocando que más ataques tengan lugar. En este sentido, se debe lograr el cálculo exacto del costo de los incidentes de seguridad para justificar los recursos asignados y evitar que ataques mayores sean realizados.

Recientemente se ha observado que, ya sea por necesidad o por conciencia, algunas organizaciones en México ya cuentan con el puesto de *Oficial de Seguridad*[126] en su organigrama, así como un área específicamente dedicada a desarrollar e implementar políticas y procedimientos para asegurar los sistemas de cómputo. Se considera que el sector que ha realizado con mayor velocidad estos cambios es el financiero, debido a que es el más vulnerable a ataques, intrusiones o robos de información.

Otro fenómeno que también esta tomando lugar es que cada vez más organizaciones se dedican a ofrecer servicios de consultoría en algún área de la seguridad informática; esto es provocado por la creciente necesidad de los gobiernos, instituciones educativas, civiles y privadas por asegurar sus sistemas de cómputo. Sin embargo, las empresas consultoras utilizan tecnología y servicios de especialistas extranjeros para realizar sus proyectos, lo que pone a nuestro país en seria desventaja.

[126] Experto en seguridad informática que se encarga de implementar y administrar políticas, mecanismos y servicios de seguridad dentro de una organización.

De hecho, muchas de estas consultorías se convierten solo en “representantes” de marcas extranjeras, dedicándose únicamente a comercializar sus productos y no a dar una asesoría adecuada a sus clientes. Incluso, algunos de estos negocios llegan a caer en charlatanería al ofrecer productos de seguridad “que lo resuelven todo” y que al final resultan inadecuados a las necesidades de sus clientes, ya que son ofrecidos (y vendidos) sin ninguna planeación ni estudio previo. De ahí que muchos sectores pidan honestidad a las empresas que ofrecen servicios de consultaría en seguridad informática.

Para tratar de contrarrestar estos problemas, algunas instituciones de educación superior, como la UNAM, han incluido materias de seguridad informática dentro de sus planes de estudios, así mismo, imparten cursos de actualización y capacitación dirigidos a profesionales y a estudiantes que deciden especializarse en el área. En este sentido, se ha observado que en los últimos meses se ha incrementado el número de personas y organizaciones que deciden capacitarse en esta área, lo que sin duda, redituará en una mayor difusión de la cultura informática y en generar una planta de especialistas de mayor cantidad y calidad.

Sin embargo, y a pesar de estos esfuerzos, todavía es insuficiente el número de profesionales especializados en el área, ya sea para impartir cátedra dentro de las universidades o prestando sus servicios como oficiales de seguridad en una organización. Mas aún si se toma en cuenta que existe también una contraparte muy activa, y es que los delincuentes informáticos han mejorado de manera notable sus técnicas de ataque, lo que les ha permitido lograr ataques exitosos que han resultado muy costosos, tanto a la economía como a la reputación de las instituciones afectadas.

En este sentido, en México se creó la Policía Cibernética como una división de la Policía Federal Preventiva (PFP), que entre sus funciones están el realizar acciones que disminuyan la incidencia de delitos cometidos en Internet o usando medios informáticos; entre los delitos más comunes se encuentran: pedofilia, pornografía, prostitución y tráfico de personas, fraude cibernético, piratería de software, intrusión a sistemas de computo, venta de armas y drogas por Internet y el ciberterrorismo[127]. Sin embargo, sus funciones son aun muy acotadas y no se le permite realizar labores de investigación y seguimiento a la delincuencia.

Otro aspecto que sin duda influye a la labor de persecución de delitos informáticos es que no existe una legislación en la materia, ya que estos delitos no están aun tipificados en nuestro país, provocando que, cuando un delincuente llega a ser detenido por cometer alguno de estos ilícitos, sea procesado legalmente por otros tipo de falta.

Todo lo anterior puede contrarrestarse si el Poder Legislativo toma acciones concretas para realizar adiciones a las leyes existentes (o crear nuevas) para cubrir el vacío que existe en cuanto a seguridad y delitos informáticos, ya que las leyes actuales en la materia son incompletas, poco claras o no existen. Así mismo, se deben crear mecanismos y acuerdos para mantener la cooperación con otros países para perseguir y castigar delincuentes que realizan delitos informáticos a nivel internacional.

[127] Fuente: www.ssp.gob.mx

De hecho, para muchos gobiernos en distintos países, los sistemas de cómputo son fundamentales para la seguridad de las instituciones y del país mismo; por ello, catalogan a la seguridad informática como un *arma de guerra*, de manera que sus leyes tipifican y castigan severamente los delitos informáticos, al mismo tiempo que mantienen acuerdos y relaciones estratégicas para perseguir y castigar a los delincuentes en diversos países.

Los avances en materia legal se han dado debido a que, los países que ya cuentan con legislaciones en seguridad han notado que los delincuentes informáticos tienen una cooperación más estrecha para generar e intercambiar información, que los mismos gobiernos. Un reto adicional a los ya planteados es la cooperación internacional, para crear y homologar leyes con respecto a delitos informáticos, así como en compartir técnicas de investigación y combate a estos ilícitos.

Como se menciona en diversas secciones de este trabajo, la seguridad informática distingue dos ámbitos bien definidos: los especialistas en seguridad, encargados del sistema en su conjunto, y el usuario de servicios de cómputo que se preocupa por su propia información.

En un futuro muy próximo será muy importante que el usuario también se capacite y se involucre en cuestiones de seguridad, ya que él forma el eslabón mas débil dentro de la cadena que conforma la seguridad; se espera además, que los ataques se enfoquen al usuario individual y no tanto los sistemas de computo. Por ello, es necesario buscar mayor difusión de la cultura de la seguridad informática, que desarrolle conciencia a todos los niveles; así como contar con mayor capacitación y especialización de parte de todos los involucrados.

ÍNDICE DE FIGURAS

Índice de Figuras.

Capítulo I.

Capítulo 2.

Capítulo 3.

Capítulo 4.

Capítulo 5.

Capítulo 6.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS:

[1] Baker, Richard H.
"Computer Security Handbook"
2nd. Edition, First printing
Ed. Tab Professional and Reference Book, 1991, USA
ISBN 0-8306-7295-2

[2] Bauer, F.L.
"Decrypted Secrets, Methods and Maxims of Cryptology".
Ed. Springer-Verlag, 1996.
ISBN 3-540-42674-4

[3] Black, Uyless
"Internet Security Protocols; Protecting IP Traffic"
Ed. Prentice Hall Series PTR, 2000, New Jersey, USA
ISBN 0-13-014249-2

[4] Burger, Ralf
"Computer Viruses, a High-Tech Disease"
3rd. Edition, April 1989
Ed. Abacus Data Becker, Dusseldorf, Germany
ISBN 1-55755-043-3

[5] Ferreyra Cortés, Fernando
"Virus en las Computadoras"
2a. Edición,
Ed. Macrobit Corp., Miami, Fl. USA. 1991
ISBN 0-939573-83-0

[6] Fisch, Erik A.; White, Gregory B.
"Secure Computer and Networks: Ananalisys, Design and Implementation"
Ed. CRC Press LLC, Boca Raton, USA, 2000
ISBN 0-8493- 1868-8

[7] Garfinkel, Simpson.
"PGP: Pretty Good Privacy".
O'Reilly and Associates, Inc., Sebastopol, CA. 1995.
ISBN 1-56592-098-8

[8] Gasser Morrie,
"Building a Secure Computer System"
Van Nostrand Reinhold, New York, 1998.
ISBN 0-442-23022-2

[9] Gratton, Pierre
"Protección Informática en datos, programas, en gestión y operación, en equipos, en redes, en Internet".
Ed. Trillas, México, 1998
ISBN 968-24-3438-6

[10] Hoffman, Lance J.
"Security and Privacy in Computer System"
Ed. Melville Publishing Company, Los Angeles, USA, 1973
ISBN 0-471-40611-2

[11] Kaufman, Charlie; Perlman, Radia; Speciner, Mike
"Network Security: Private Communication in a Public World"
Ed. PTR Prentice Hall, 1995, New Jersey, USA
ISBN 0-13-061466-1

[12] Mallén Fullerton, Guillermo M.
"Virus Computacionales, enfoque objetivo"
Conacyt, México, 1994
ISBN 968-823-259-9

[13] Menezes A.J., Van Oorschot P.C., Vanstone S.A.,
"Handbook of Applied Cryptography"
Ed. CRC Press, 1997
ASBN 0-8493-8523-7

[14] Peltier, Thomas R.
"Information Security Policies, Procedures and Standars"
Ed. Averbach, 2002, Boca Raton, USA
ISBN 0-8493-1137-3

[15] Pflegeer, Charles P.
"Security in Computing"
Second Edition
Ed. Prentice Hall PTR, Upper Saddle River, NL 07458, 1996
ISBN 0-13-337486-6

[16] Schneier, Bruce.
"Applied Cryptography"
2nd edition.
New York, NY; John Wiley and Sons, Inc., 1996.
ISBN 0-471-11709-9

[17] Stallings, William
"Network and Internetwork Security, Principles and Practice"
Ed. Prentice Hall, 1995
ISBN 0-02415483-0

[18] Stallings, William.
"Practical Cryptography for Data Internetworks".
IEEE Computer Society Press, 1996. Los Alamitos, CA.
ISBN 0-81-867140-8

[19] Stallings, William.
"Protect Your Privacy: The PGP User's Guide".
Prentice Hall PTR, Englewood Cliffs, N.J., 1995.
ISBN 0-13-185596-4

[20] Summers, Rita C.
"Secure Computing: threats and safeguards"
McGraww-Hill 1997
ISBN 0-07-069419-2

[21] Tanenbaum, Andrew S.
"Computer Networks, Fourth Edition"
Ed: Prentice Hall, New Jersey, USA, March 2003
ISBN 0-13-066102-3

[22] Tapia, Ricardo.
***"Las Células de la Mente"*.**
Serie *La Ciencia desde México*, Número 30.
Ed. Fondo de Cultura Económica, México, D.F., 1995
ISBN 968-162545-5

[23] Tudor, Jan Killmeyer
"Information Security Architecture: an Integrated Approach to Security in Organization"
Ed. Averbach, Boca Raton, USA, 2000
ISBN 0-8493-9988-2

INTERNET:

Adaware
www.lavasoftusa.com
www.safernetworking.org/en/index.html

Anti Phising
http://www.antiphishing.org/crimeware.html

Archivo Portable Ejecutable
http://win32assembly.online.fr/pe-tut1.html
http://www.csn.ul.ie/~caolan/publink/winresdump/winresdump/doc/pefile.html

Biométricos
www.biometrics.org/
http://homepage.ntlworld.com/avanti/whitepaper.htm
http://secinf.net/
www.cesg.gov.uk/biometrics/pdfs/
http://computer.org/itpro/
www.Finger-scan.com
www.Iris-scan.com
www.Retina-scan.com
www.Hand-scan.com
www.Voice-scan.com
http://www.jamejamdaily.net/shownews2.asp?n=26454&t=com
www.auscert.org.au

Buenas Prácticas
http://resnet.uci.edu/security/bestpractices.asp

Certificados Digitales
Verisign www.verisign.com

Control de Acceso
http://www.blanchard739.com/index2.htm

Core Wars
http://www.corewars.org/

Costos
http://www.nemx.com/products/securexchangeantivirus/index.asp
http://www.cmsconnect.com/Marketing/viruscalc.htm
http://www.cmsconnect.com/Marketing/CalcMain.htm
http://www.software602.com/products/ls/roi.html
http://www.idc.com/getdoc.jsp?containerId=LA1530
http://www.educause.edu/content.asp?page_id=666&ID=CSD2813&bhcp=1
http://www.cmsconnect.com/Marketing/viruscalc.htm

http://www.cmsconnect.com/Marketing/CalcMain.htm
http://www.software602.com/products/ls/roi.html
http://staff.washington.edu/dittrich/misc/faqs/incidentcosts.faq
http://www.cmsconnect.com/Marketing/viruscalc.htm
http://online.securityfocus.com/infocus/1592
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci956157,00.html
http://www.usenix.org/publications/login/1999-6/icamp.html
http://www.securityfocus.com/infocus/1592
http://www.pcworld.com/news/article/0,aid,118648,00.asp
https://www.icsalabs.com

Criptografía
http://cryptographer.biography.ms/
http://www.finecrypt.net
http://www.nih.gov/science/computers/amg/secrpt.htm
http://www.computercops.biz/article1432.html
http://www.fas.org/irp/program/disseminate/ddn.htm
http://www.acm.org/awards/turing_lectures_project/turing/S/s-pp/shamir_1files_files/800x600/Slide1.html
http://www.acm.org/awards/turing_citations/rivest-shamir-adleman.html
http://www.rsasecurity.com/rsalabs/node.asp?id=2248
www.gocsi.com
www.info-sec.com

Criterios Comunes
http://www.commoncriteria.com/cc.html

Desarrollo del Cerebro
http://preschoolrainbow.org/brain-growth.htm
http://www.brocku.ca/stutter/frpgs/lobe.html
http://www.vh.org/adult/provider/anatomy/BrainAnatomy/5Hemispheres.html

Diccionario de la Real Academia Española
http://www.rae.es

Discos Duros
www.dewassoc.com/kbase/hard_drives/hard_disk_sector_structures.htm

Encuesta de Seguridad en México
www.ey.com

Estadísticas
http://www.inegi.gob.mx/inegi/contenidos/espanol/acerca/inegi324.asp?c=324
http://www.inegi.gob.mx/est/default.asp?c=3421
http://www.razonypalabra.org.mx/anteriores/n43/oislas.html

Esteganografía
http://www.outguess.org/

Finanzas
http://www.itfacts.biz/
http://www.banksafeonline.org.uk/
http://www.bankers.asn.au/
www.ey.com

Firewalls
http://www.serverworldmagazine.com/compaqent/2000/07/firewall.shtml

Historia de la Computación
http://www.columbia.edu/acis/history/la36.html
http://www.acabtu.com.mx/tech/virus/cronologia.html

Lenguajes y Escritura
http://www.crystalinks.com/languages.html
http://jom-emit.cfpm.org/1998/vol2/vaneechoutte_m&skoyles_jr.html

Mapa Internet
http://www.grc.com/dos/theinternet.htm

Pharming
https://www.pharming.org/index.jsp
http://www.crime-research.org/news/20.04.2005/1166/

Phising
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=132
http://secunia.com/multiple_browsers_idn_spoofing_test/ http://www.paypal.com/
http://www.hispasec.com/unaaldia/2325

Políticas
http://www.sans.org/resources/policies/#name

Redes de Computadoras
http://www.netlib.org/hence/
http://www.zdnet.com.au/itmanager/technology/story/0,2000029587,20273903,00.htm
http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm/b/67.htm
http://www.linuxfocus.org/English/July2002/article245.shtml
http://www.radium.ncsc.mil/tpep/library/rainbow/
http://www-106.ibm.com/developerworks/linux/library/l-share2/

Seguridad
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=132

Skytale
http://de.wikipedia.org/wiki/Skytale

Spam
www.nucleusresearch.compress_releases/prspam2.HTML
www.adnuker.com/index.htm
www.ashampoo.com
www.pctools.com/spam-monitor

Spyware
www.safer-networking.org/en/index.html
www.pctools.com
http://www.8e6.com/network_world_spyware_form.htm
www.microsoft.com/athome/security/spyware/software/default.mspx

Virión
http://biodynamics.indiana.edu/

Virus Biológicos
http://biodynamics.indiana.edu/

Virus Informáticos
http://www.cdt.org/security/dos/000223senate/cohen.html
http://www.perantivirus.com/sosvirus/general/tunel.htm
http://www.perantivirus.com/sosvirus/general/
http://www.vsantivirus.com/fdisk-mbr.htm
http://www.nondot.org/sabre/os/files/Booting/mbr.txt
http://www.dewassoc.com/kbase/hard_drives/hard_disk_sector_structures.htm
http://www.nondot.org/sabre/os/files/Partitions/PartitionTables.txt
http://support.microsoft.com/kb/q69013/
http://vil.nai.com
http://www.avertlabs.com
www.techweb.com
http://www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml
http://www.nist.gov/public_affairs/siteindex.htm
http://antivirus.about.com/?once=true&
http://csrc.nist.gov/virus/
www.vsantivirus.com
http://computer.howstuffworks.com/virus.htm
http://www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml
http://www.alerta-antivirus.es/index.php
http://www.antivirus.com/pc-cillin/vinfo/safe_computing/
http://www.antivirus.com/pc-illin/vinfo/safe_computing/zipped_registry.htm
http://www.vsantivirus.com/otros.htm#esp
http://www.vsantivirus.com/faq-vbs.htm
http://virusattack.xnetwork.com.ar/documentos/
http://windowsupdate.microsoft.com

http://www.vsantivirus.com/consejos-outlook.htm
http://www.vsantivirus.com/20vul.htm
http://virusattack.xnetwork.com.ar/parches/
http://www.vsantivirus.com/15-10-01.htm
http://www.zonavirus.com/
http://www.virusbtn.com/
http://www.malware.com/
http://www.securityfocus.com
http://en.wikipedia.org/wiki/Malware
http://www.acabtu.com.mx/tech/virus/cronologia.html
http://www.wired.com/news/infostructure/0,1377,49681,00.html
http://www.computereconomics.com/
http://software.silicon.com/malware
http://www.networkworld.com/topics/virus.html
http://www.ciac.org/ciac/ciac_virus_info.html
https://www.icsalabs.com/icsa/topic.php?tid=cfe0$3d83e732-011a28d6$5ac9-0f77e15b
http://www.virusbtn.com/news/virus_news/2005/index.xml

DIARIOS:

"El Universal"
Sección de Computación
Lunes 21 de febrero de 2005, pp. 1

"El Economista"
Sección "IT"
Lunes 17 de Febrero de 2003, pp. 4
Lunes 14 de Abril de 2003, pp. 7
Lunes 1 Agosto de 2005, pp. 4
Lunes 8 de Agosto de 2005, pp. 3, 4
Lunes 16 de octubre de 2006, pp. 6

Sección "Empresas y Negocios"
Miércoles 12 de octubre de 2005, pp. 28

Sección "Nuestro Tema"
Lunes 21 de Agosto de 2006, pp. 4
Martes 22 de Agosto de 2006, pp. 3
Lunes 9 de enero de 2006, pp. 14

Sección "Pymes"
Miércoles 12 de Octubre de 2005, pp. 37
Lunes 16 de Octubre de 2006, pp. 48

Sección "Valores y Dinero"
Lunes 3 de enero de 2005, pp. 7
Martes 4 de enero de 2005, pp. 47
Viernes 17 de junio de 2005, pp. 13
Lunes 10 de Octubre de 2005, pp. 56

Numero Especial
Año I, pp. 1-4

REVISTAS

¿Cómo ves?
Dirección General de Divulgación de la Ciencia, UNAM
Año 6, Número 69, pp. 10
"Seguridad en Internet"
Por: Daniel Martín Reina

ContHACKto.net
Know-How Editores
Año 1, Volúmen 1, Número 0
Agosto / Septiembre de 2005
"La importancia de llamarse Hacker", pp. 3
"Introducción a la Criptografía Cuántica", pp. 10

Muy Interesante
Editorial Televisa
Año XX, Año 2, 1 de Febrero de 2003
"La amenaza de los nuevos virus", pp. 16

Net Times Communications
Grupo Editorial RIM
Mayo 1999 Año 2 Número 26
"Detección de Ataques al momento", pp. 1
Por: Anita Karvé