UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Propuestas para impulsar la seguridad informática en materia de educación

TESIS PROFESIONAL
que para obtener el título de
INGENIERO EN COMPUTACIÓN

PRESENTA:
MAGDALENA REYES GRANADOS

DIRECTOR DE TESIS:
M. en C. Jaquelina López Barrientos

Ciudad Universitaria, Octubre 2011

AGRADECIMIENTOS

A mi mamá, por ser la amiga y compañera que me ha brindado todas las enseñanzas para crecer como persona, por el tiempo que me dedicaste, por tu paciencia, por todo tu amor y entrega, por todo el apoyo incondicional que me brindaste a lo largo de mi carrera. Gracias Mami por todos los sacrificios que hiciste para que yo pudiera culminar mis estudios. Te amo con todo mi corazón mamita.

A mi hija Hannah Sophia, aunque todavía no sabes leer, un día lo aprenderás. Gracias por llegar a mi vida y regalarme momentos maravillosos. Gracia por acompañarme a la realización de esta Tesis. Gracias por apagarme la computadora cuando yo trabajaba, gracias bebé por ser mi motorcito para salir adelante. Te Amo mi chiquita hermosa.

A mi hermana Mary, quien me apoyó en todo momento para que yo saliera adelante. Gracias por confiar en mí y por la ayuda que me brindaste cuando la necesitaba.

A mi hermana Sandra, por todo el apoyo que me brindó, por sus valiosos consejos, por acompañarme en mis desvelos y sobre todo por creer en mí.

A mis amigos, Sandra y Adrián, porque estuvieron conmigo en todo momento, por sus consejos y por todo su apoyo incondicional.

A Jaquelin, por ser mí maestra, mi directora de tesis. Gracias por toda su paciencia y su valioso tiempo que me brindó, por sus conocimientos que me han sido de gran ayuda. Gracias por todo su apoyo para la culminar este trabajo y sobre todo por los consejos que me dio para salir adelante.

A mis sinodales, por el tiempo que me dedicaron para leer este trabajo y por sus críticas y comentarios, ya que me sirvieron para mejorarlo.

Magdalena Reyes Granados

PROPUESTAS PARA IMPULSAR LA SEGURIDAD INFORMÁTICA EN MATERIA DE EDUCACIÓN

Índice general

Introducción

Índice de Gráficas

Gráficas

Capítulo 1

Capítulo 2

Capítulo 3

Índice de Tablas

Capítulo 1

Capítulo 2

Capítulo 3

Capítulo 4

Índice de Figuras

PROPUESTA PARA IMPULSAR LA SEGURIDAD INFORMÁTICA EN MATERIA DE EDUCACIÓN

Panorama general de la seguridad informática

En las últimas décadas la tecnología ha ido avanzando constantemente, se ha visto reflejado en la vida cotidiana de las personas, por ejemplo, al momento de realizar un pago, consultar estados de cuenta, realizar compras, consultar información de interés personal, entre otros. Todo esto ahora se realiza a través de Internet, que se ha convertido en la herramienta de uso común en las personas debido a la facilidad que brinda para comunicarse a cualquier parte del mundo a un costo muy bajo.

Las empresas hoy en día están obligadas a mantener esta tecnología para la obtención de beneficios y mejorar su productividad, por lo tanto, la seguridad informática se ve en la necesidad de ir en paralelo con este avance tecnológico y al mismo tiempo se manifiesta el incremento de los delitos en la red, van desde el engaño, soborno, extorsión, estafas mediante phishing (robo de identidad), creación de falsos antivirus, denegación de servicios, spam, virus, gusanos, entre otros, provocando grandes daños a los equipos de comunicaciones, causando enormes pérdidas a las empresas que hayan sido víctimas de algún ataque en cibernético.

Por lo antes mencionado es conveniente concientizar a las empresas sobre la importancia de mantener un buen sistema de seguridad en los equipos de comunicación que almacenan y distribuyen información a cualquier parte del mundo, derivado de la existencia de amenazas que van desde ataques por suplantación de servicio de páginas web, robo de información confidencial, ataques masivos a páginas web, entre otros. Si no se toman las medidas pertinentes, se está poniendo en riesgo, tanto los activos de la empresa como su reputación, lo que puede causar grandes pérdidas económicas.

Otro factor importante para mantener un buen sistema de seguridad informática es el presupuesto que proporcionan las empresas para esta área, se sabe que actualmente existen

algunas empresas que no destinan el suficiente presupuesto a la seguridad informática debido a que consideran que por ser poco conocidas, los hackers no se fijarían en ellos como punto blanco de ataque, lo cual es un grave error, ya que el hacker busca sistemas vulnerables y dependiendo de los intereses que persiga será el tipo de red y sistema que serán adecuados para sus fines no importando el lugar físico en el que se encuentren tanto la víctima como el hacker.

La mayoría de las empresas consideran que la seguridad informática es un gasto y no una inversión porque aparentemente no ven reflejado en cuestión monetaria sus ganancias, únicamente se puede observar mediante herramientas de monitoreo de red los intentos de ataques que éstas tienen. De esta manera se obtienen los análisis y se realizan estadísticas que determinan la situación y los principales ataques a los que se está expuesto, por ello, se vuelve indispensable la difusión acerca de la importancia de la seguridad informática, ya que de otra forma cuando la empresa se percata de alguna acción sospechosa resulta ser, en la mayoría de los casos demasiado tarde. Si no se invierte en seguridad por considerar que no vale la pena, las consecuencias de haber sufrido un ataque y repararlo en su mayoría resultan ser muy costosas llegando a provocar, incluso la quiebra de la empresa.

Es conveniente hacer conciencia en el personal que labora en las empresas sobre el valor de la información, para evitar lo que se conoce hoy en día como el ataque de Ingeniería Social, el cual consiste en la obtención de información confidencial a través de la manipulación de usuarios legítimos, por eso se dice que el talón de Aquiles de cualquier red lo componen los usuarios que la integran, de hecho el *Informe Anual sobre Seguridad* realizado por la empresa CISCO correspondiente al año 2008 sobre el elevado costo de las amenazas internas que existen en los principales países a nivel mundial. Este informe señala que el 39% de los profesionales de TI están más preocupados por las amenazas provenientes de sus propios empleados que por la de los piratas informáticos externos. Asimismo, dicho informe presenta cifras alarmantes en el sentido de que el 43% de los profesionales de TI afirmó que no crea conciencia sobre aspectos de seguridad informática en los empleados como es debido.

Es necesario se tenga claro el rumbo que debe tomar la seguridad informática en el mundo, particularmente con base en nuestros intereses centraremos el presente estudio en nuestro país, a fin de hacer un plan nacional que considere por una parte la formación de recursos humanos altamente capacitados para afrontar los retos que se avecinan, de igual forma la inversión que debe realizarse en materia de desarrollo tecnológico para proteger los sistemas de cualquier tipo de amenaza, garantizando que los equipos de comunicación funcionen correctamente con el menor riesgo posible basándose en los principios fundamentales de la seguridad informática que son la **Confidencialidad** (asegura que sólo las personas autorizadas puedan acceder a la información), **Disponibilidad** (asegura que la información esté accesible siempre que las personas autorizadas la necesiten) e **Integridad** (asegura que la información sea completa y precisa, solamente modificable por el personal autorizado) de la información.

Objetivo General

- Realizar una investigación que permita estudiar, analizar y determinar la situación actual de la seguridad informática en México y su contraste a nivel internacional.

Objetivos Particulares

- Conocer el desarrollo de la seguridad informática a nivel mundial.
- Comprender el desarrollo de la seguridad informática en México y su relación con el mundo.
- Identificar las principales amenazas y vulnerabilidades a las que se enfrentan las organizaciones a nivel nacional e internacional.
- Determinar las tendencias existentes en materia de seguridad informática en México.
- Dar a conocer los resultados de la investigación realizada.
- Proponer un plan de acción para impulsar la seguridad informática en cuanto a educación y desarrollo tecnológico desde las universidades.

Capítulo 1
Definiciones e historia de la seguridad informática

Desde el surgimiento de la raza humana en el planeta, la información ha estado presente bajo diversas formas y técnicas. El hombre buscaba la manera de representar sus hábitos y costumbres en diversos medios para que pudieran ser utilizados por él y por otras personas. La información valiosa era registrada en objetos preciosos y sofisticados, pinturas magníficas, entre otros, que se almacenaban en lugares de difícil acceso y sólo las personas autorizadas accedían a ella.

En la actualidad la información es el objeto de mayor valor para las empresas. El progreso de la informática y de las redes de comunicación nos presenta un nuevo escenario, donde los objetos del mundo real están representados por bits y bytes, que ocupan lugar en otra dimensión y poseen formas diferentes de las originales, no dejando de tener el mismo valor que sus objetos reales, e incluso en muchos casos, llegando a tener un valor superior. Por ello la seguridad informática es muy importante ya que afecta directamente a gobiernos, institutos, empresas e individuos.

1.1 Conceptos Básicos

El mundo de la seguridad informática es amplio y complejo, para ello es indispensable dar una definición de los términos más utilizados en este trabajo de investigación. Se define la palabra *seguridad*: "*Viene del latín seguritas, se refiere a la cualidad de seguro, es decir, aquello que está exento de peligro, daño o riesgo. Algo seguro es algo cierto. La seguridad por lo tanto es una certeza*".[1]

Esta definición es muy general y me parce importante mencionar que la *seguridad* se encuentra presente de manera consciente o inconscientemente en la vida cotidiana de las personas. Por ejemplo, al salir de los hogares se toman las debidas precauciones de mantener cerradas puertas y ventanas para evitar que algún individuo ajeno a éste pueda ingresar, asimismo se verifica que no quede algún electrodoméstico encendido que pueda provocar un accidente, se revisan que las llaves de agua o gas queden completamente cerradas para evitar posibles fugas que llegasen a provocar inundaciones e incendios. Todo esto se realiza con el objetivo de mantener la mínima posibilidad de padecer cualquier tipo de contingencia.

El término de *seguridad* implica pensar en confianza, por ejemplo, las personas tienen la confianza de estar en algún lugar porque se sienten seguros, si fuese lo contrario, buscarían la forma de obtenerla y es cuando se hace conciencia sobre lo que se debe de hacer para mantenerla al máximo.

Por lo antes mencionado se tiene una mejor visión del significado del término seguridad, para el caso particular de este trabajo de investigación, el estudio de seguridad en lo que hoy en día se conoce como *seguridad informática*. Pero, antes de entrar en materia se define el concepto de *informática: "Es el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores"*.[2]

[1] http://definicion.de/seguridad/
[2] Informática y Comunicaciones en la Empresa de Carmen de Pablos. Madrid, España. 2004 p.33 y 34.

Este manejo automático de la información ha propiciado y facilitado la manipulación de grandes cantidades de datos para su rápida ejecución. La informática se encarga de estudiar lo que los programas (software) son capaces de hacer y se toma en cuenta la eficiencia en la organización y almacenamiento de datos, así como de la comunicación entre programas, personas y máquinas.

1.1.1. Definición de Seguridad Informática

Se define a la *seguridad informática* de diferentes formas:

- *"Disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático".*[3]
- *"Consiste en aquellas prácticas que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida".*[4]

De las cuales me parece importante destacar que para el presente trabajo se entenderá por *seguridad informática* a la disciplina que se encarga de proteger y resguardar toda la información que se encuentra almacenada, que es generada, procesada y transportada a través de los sistemas y equipos de comunicación.

La *seguridad informática* se ha convertido en un factor de gran importancia principalmente en las organizaciones, derivado de la necesidad de mantener protegida la información que se encuentra en los dispositivos electrónicos así como de los usuarios que la manejan.

En las organizaciones existen ciertas normas que ayudan a mantener una mayor seguridad en los sistemas de información, estas normas se conocen con el nombre de ***Políticas de Seguridad*** y se definen como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema, indica en términos generales lo que

[3] http://definicion.de/seguridad-informatica/
[4] http://www.definicionabc.com/tecnologia/seguridad-informatica.php

está y lo que no está permitido. En términos generales se puede decir que una política de seguridad puede ser:

- Prohibitiva, es decir, todo lo que no está expresamente permitido está denegado.
- Permisiva, es decir, todo lo que no está expresamente prohibido está permitido.

Para ello existen normas que ayudan a las empresas a la creación de sus políticas de seguridad, las cuales me parece interesante describir:

- **La Norma ISO/IEC 27001 (International Organization for Standardization/International Electrotechnical Comission):** *"Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados".*[5]
- **La Norma ISO/IEC 27002:** *"Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios".*[6]

Los beneficios de contar con estas normas es que ayudan a establecer de manera clara y ordenada, una buena metodología de gestión en materia de seguridad de la información, así como la reducción de riesgos en cuanto a la pérdida, robo o corrupción de la información garantizando que los usuarios tengan acceso de manera segura. Es por ello que se realizan auditorías tanto externas como internas ya que ayudan a identificar las

[5] http://www.iso27000.es/iso27000.html#section3b
[6] http://www.iso27000.es/iso27000.html#section3b

posibles debilidades del sistema y lo más importante es que incrementa el nivel de concientización del personal que labora en las empresas.

1.2 Principios

El objetivo de la seguridad informática es proteger los activos (todo aquel recurso del sistema de información necesario, para que la empresa funcione correctamente) y para ello se basa en tres principios básicos los cuales son:

- **Integridad: "***Significa que el sistema no debe modificar ni corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados sin que se haya producido ninguna modificación, adición o borrado"*.[7]

Es importante destacar que una información íntegra es una información que no ha sido alterada de manera indebida y cuando esto ocurre significa que los datos han perdido su valor original.

Los usuarios deben tener la seguridad de que la información que están obteniendo, leyendo y trabajando es exactamente la misma que fue colocada desde un principio, es decir, que sea la información original, si ésta sufre alteraciones puede ocasionar grandes conflictos perjudicando la comunicación y la toma de decisiones en las organizaciones.

La información se altera de diversas formas:

- *Alteración de contenido en los documentos:* Se realizan inserciones o sustituciones de partes de su contenido.

[7] http://www.unsl.edu.ar/~tecno/redes%202008/seguridadinformatica.pdf

- *Alteración en los elementos que soportan la información:* Se realizan alteraciones en la estructura física y lógica donde la información se encuentra almacenada, por ejemplo, en los equipos de cómputo y en los servidores.

Es necesario tener la certeza de que, únicamente las personas autorizadas pueden realizar alguna modificación en la forma y contenido de la información garantizando la integridad de ésta.

- **Confidencialidad: "***La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas o procesos no autorizados puedan acceder a la información almacenada en él".*[8]

La información que se intercambia entre individuos y empresas no siempre deberá ser conocida por todo el mundo, debido a que se puede hacer un uso inapropiado de ésta causando múltiples daños a las organizaciones o individuos que manejan la información. Únicamente la o las personas autorizadas podrán conocer el contenido de la información que haya sido enviada, si la información es confidencial, quiere decir, que es secreta y no deberá de ser divulgada a entes no autorizados.

Es necesario que las empresas tomen conciencia acerca de la importancia de mantener sus sistemas de información de manera confidencial, garantizando que los datos que se encuentran en los equipos de comunicación lleguen a su destino sin haber sido interceptados por otros usuarios.

Por ejemplo si los usuarios revelan sus contraseñas o sus números confidenciales, se corre el riesgo de que alguien pueda hacer un uso indebido de la información, puesto que se tiene el acceso fácilmente, a esto se le conoce como ingeniería social y un ataque muy común es el ataque de phising que consiste en conseguir información confidencial para la obtención de un beneficio, como la realización de fraudes bancarios. En el siguiente capítulo se explica con mayor detalle los principales ataques que afectan a los sistemas de cómputo.

Una vez que se asegura que la información llegue a los destinatarios o usuarios correctos se debe garantizar que esa información llegue en el momento deseado a lo que se conoce como:

[8] http://www.unsl.edu.ar/~tecno/redes%202008/seguridadinformatica.pdf

- **Disponibilidad: "***Significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de falla".*[9]

La disponibilidad permite que la información se pueda utilizar cuando sea necesario, estando al alcance de las personas autorizadas. Así, la información debe ser accesible en forma segura para que se pueda usar en el momento en que se solicita, garantizando la integridad y confidencialidad de ésta.

Esto conlleva a que los equipos de comunicación deben de estar funcionando correctamente y de manera segura, en caso contrario se está expuesto a sufrir cualquier tipo de ataque teniendo como resultado daños a la reputación y consecuencias legales, entre otros. Para que la información esté disponible es recomendable que las empresas u organizaciones cuenten con más de un respaldo de la información para mantenerla siempre disponible.

Es pertinente que las organizaciones cuenten con un departamento encargado de la seguridad informática, llevando a cabo las siguientes actividades como:

- **Análisis de Riesgo:** Proceso mediante el cual se identifican las amenazas y las vulnerabilidades en una organización, valorando su impacto y la probabilidad de que ocurran.
- **Plan Integral de Seguridad Informática:** Se definen los lineamientos de la planeación, el diseño e implantación de un modelo de seguridad cuyo objetivo es proteger la información y los activos de la organización, garantizando la confidencialidad, integridad y disponibilidad de los datos.
- **Políticas de Seguridad:** "*Requisitos definidos por los responsables de un sistema, que indica en términos generales, que está y que no está permitido en el área de seguridad durante la operación del sistema".*[10]
- **Clasificación de Activos Informáticos:** Se debe mantener un listado detallado de los activos de información como su localización, clasificación de seguridad y riesgo, propietario, grupo de activo al que pertenece, entre otros.

[9] http://www.unsl.edu.ar/~tecno/redes%202008/seguridadinformatica.pdf
[10] http://www.segu-info.com.ar/politicas/polseginf.htm

- **Auditorías:** Se provee el aseguramiento independiente de la administración en relación a la efectividad de los objetivos de la seguridad de la información.

Por lo antes visto se puede observar que la seguridad informática se basa en tres principios fundamentales los cuales son: la Integridad, Disponibilidad y Confidencialidad. Estos ayudan a mantener un nivel de seguridad acorde a las necesidades de las organizaciones o de las personas que la requieran, si no se tuvieran en cuenta estos principios, realmente no se tendría un buen sistema de seguridad ya que cualquier individuo tendría acceso a la información, realizando alguna modificación o anomalía que afecte a las organizaciones, por ello es indispensable contar con un departamento del área de seguridad informática el cual se encargue de organizar todos los activos de la empresa, llevando a cabo un análisis para determinar las posibles anomalías que se presenten, de tal manera que ayude a prevenirlas y así mantener un buen sistema de seguridad de la información.

1.3 Antecedentes de la Seguridad Informática a nivel Nacional e Internacional

Es importante conocer el surgimiento de la historia de la tecnología, para entender la situación a la que nos enfrentamos hoy en día, por lo que resulta interesante conocer cuántas cosas tuvieron que suceder para llegar hasta lo que hoy tenemos, quiénes fueron las personas que idearon e inventaron los diversos desarrollos tecnológicos e incluso determinar hacia dónde se dirige la tecnología y por supuesto hacia dónde va la seguridad informática.

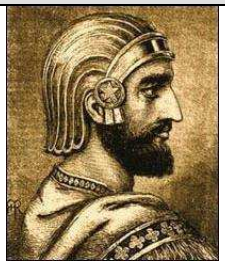
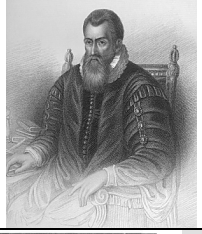
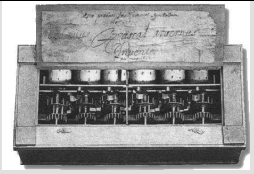
Para ello, fue indispensable optimizar los recursos tecnológicos con los que se contaba en determinada época de tal manera que se mantuviera un buen sistema de seguridad de la información.

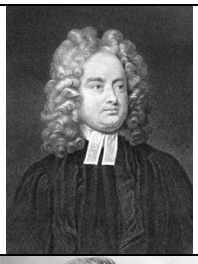
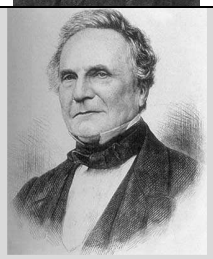
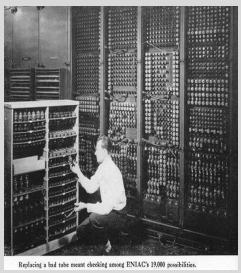
Cabe destacar que este desarrollo tecnológico de la información ha tenido consecuencias debido a que existen personas que buscan la manera de violar la integridad,

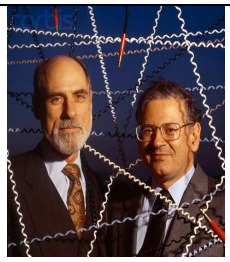
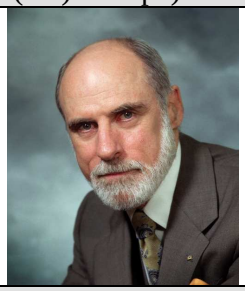
confidencialidad y disponibilidad de la información que viaja a través de los equipos de comunicación con el fin de realizar acciones indebidas y obtener beneficios personales.

Todos estos acontecimientos que se fueron desarrollando se muestran de manera cronológica en la tabla 1.1 Resulta interesante analizar cómo es que, a través de los años, se han ido logrando varios avances tecnológicos en los diversos países competitivos como Estados Unidos y Japón, cuyo objetivo principal es y seguirá siendo, mantener seguros los sistemas en donde se almacena la información, teniendo una comunicación confiable y segura entre ellos.

Tabla. 1.1 Acontecimientos internacionales que marcaron el desarrollo de la seguridad informática

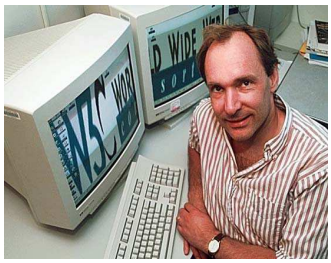
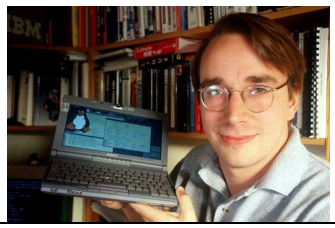
Año	Acontecimiento		Reseña
550 aC	Primer Sistema de correo		Ciro el Grande, rey de Persia, diseña el primer sistema para transmitir información por postas. Setecientos años después, los chinos también tendrán el suyo a lo grande: 50 mil caballos, 1400 bueyes, 6700 mulas, 400 carros, 6mil botes, 200 perros y 1150 ovejas.
1605	Bacon crea el Alfabeto binario		Bacon describe un modo de representar las letras del alfabeto en secuencias de cifras binarias, sucesiones de ceros y unos, fácilmente codificables y decodificables.
1614	Napier inventa los logaritmos		Descubre este concepto matemático que resultará crucial para la programación de computadoras.
1623	Las Primeras Calculadoras		Wilhelm Schickard construye la primera calculadora mecánica con poleas y engranajes de reloj. El filósofo y matemático Blaise Pascal presenta la Pascalina en 1642.

1726	La computadora de Gulliver		Jonathan Swift describe satíricamente una máquina imaginaria de bloques de madera accionada con una palanca capaz de componer discursos.
1833	Llega la primera computadora		Charles Babbage diseña un "motor analítico", una computadora programable para todo tipo de propósitos. Debido a su funcionamiento a vapor y al hecho de que todas las piezas son fabricadas a mano, el proyecto fracasa. La idea sigue.
1860	Hola, Teléfono		Antonio Meucci es el primer inventor del aparato de comunicación de voz a distancia que patenta el escocés Alexander Graham Bell en abril de 1875.
1946	Primera computadora electrónica		John Presper Eckert y John William Mauchly construyen la ENIAC (Electronic Numerical Integrator And Computer) en la Universidad de Pensilvania. Su propósito: calcular la trayectoria de proyectiles para el laboratorio de balística del ejército. Es totalmente digital. Pesa 27 toneladas, ocupa una superficie de 167m^2 y opera con 17,468 válvulas electrónicas.
1950	Computadoras conectándose con otras Computadoras	El proyecto se denomina RAND (Research And Development) y se desarrolla para facilitar el intercambio entre investigadores en inteligencia artificial.	
1958	Nace ARPA (Advanced Research Project Agency) El abuelo de Internet	Con el objetivo de impulsar la investigación y el desarrollo tecnológico con fines estratégicos y militares, EE.UU. establece la ARPA, en cuyo seno nace ARPANET, más tarde Internet.	

1961	Los paquetes de información inician su viaje		Varios investigadores desarrollan paralelamente la idea de que la información viaje en paquetes. Es decir, conjuntos limitados de datos unidos a la información necesaria para controlarlos. En este desarrollo se destacan dos personajes clave: Vinton Cerf y Robert Kahn.
1969	Atando nodos.	En 1969 se creó la primer red de computadoras entre cuatro centros de investigación que conforman históricamente los primero cuatro *hosts* de Internet que fueron SRI (Stanford Research Institute), UCLA (University of California in los Angeles), UCSB (University of California in Santa Barbara) y la Universidad de Utah. A esta red se le denominó ARPANET (red (net) de arpa).	
1970	Alguien escribe una palabra nueva: Internet		Vinton Cerf es considerado la primera persona que acuña el término Internet.
1971	El correo electrónico abre sus puertas	Ray Tomilinson, de la empresa contratada BBN, idea un programa de correo electrónico para enviar mensajes a través de la red.	
1972	¿El Primer Virus? Llega la arroba	- De repente, en las pantallas de todas las IBM 360 empieza a aparecer un mensaje: “”I’m a creeper… catch me if you can” (Soy una enredadera. ¡Atrápame si puedes!). Robert Thomas Morris es considerado el autor de este mítico virus que da lugar lógicamente, al primer programa antivirus. ¿Cómo se llamará?, algo muy lógico: “Reaper”, es decir, segadora. - Al perfeccionar su programa de correo electrónico, Ray Tomlinson rescata el antiguo símbolo @ para separar el nombre del destinatario del lugar donde se encuentra.	
1973	La conexión cruza el océano		NORSAR (NOR-wegian Seismic AR-ray), una agencia gubernamental noruega de detección sísmica, fue la primera institución europea que se conectó a la red de ARPANET. Poco después, lo hizo también el University College de Londres.
			- John Walker descubre la forma de distribuir un juego en su

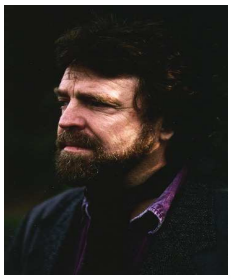
1975	Primer Troyano Bill Gates funda Microsoft		UNIVAC 1108 e inadvertidamente da origen al primer troyano de la historia llamado “Animal/Pervade”. Animal ya que consistía en que el software debía adivinar el nombre de un animal en base a preguntas realizadas al usuario. Pervade era la rutina capaz de actualizar las copias de Animal en los directorios de los usuarios, cada vez que el mismo era ejecutado. - Microsoft se dedica a desarrollar, fabricar y producir software y equipos electrónicos. A mediados de los 80 domina el mercado de los ordenadores personales con su sistema operativo MS-DOS. En el 2007 registra 80,000 empleados en más de 100 países, así como beneficios anuales superiores a los 50,000 millones de dólares.
1976	Crece una Manzana		Steve Jobs, de 21 años y Steve Wozniak, de 25, diseñan una computadora más pequeña, más barata y más fácil de utilizar que las ya existentes. Inspirado en el huerto de Oregón donde había trabajado con algunos amigos, Jobs la bautiza con el nombre de “Apple Computer”.
1977	Primera demostración del protocolo TCP/IP	El transmisión Control Protocol / Internet Protocol, abreviado TCP/IP, se caracteriza por un excelente funcionamiento. Es el único conjunto de reglas para el envío de datos que años más tarde aprobó ARPANET.	
1978	Y mañana será spam	Trescientos noventa y tres empleados de ARPANET reciben inesperadamente un correo de la compañía de ordenadores DEC invitándolos al lanzamiento de un nuevo producto. Se trata del primer antecedente del más tarde denominado spam.	
1979	Nace Usenet	Tom truscott y Jim Ellis, estudiantes de la Universidad de Duke, crean Usenet. Palabra formada con las primeras letras de Ussers Network; es decir, red de usuarios. Permite enviar y recibir mensajes (denominados artículos) a distintos grupos de	

		noticias, aportando y discutiendo sobre temas determinados.
1981	Llega la PC de IBM	 IBM presenta su PC. Un año más tarde la revista Time la colocará en el lugar del habitual “Hombre del Año”.
1982	Comienza la invasión de ratones Llega Minitel	- El primer Mouse de uso doméstico es presentado por Mouse Systemas. Sirve par ala PC de IBM. Su invención original corresponde a Douglas Engelbart y data de 1967. - Este servicio de videotexto mediante redes de teléfono es lanzado en Francia por PPt. Es considerado el servicio online más exitoso hasta el arribo de la World Wide Web.
1983	ARPANET se desmilitariza Los virus se hacen públicos TCP/IP protocolo único	- En 1983 la parte civil se separó de la parte militar de la Arpanet y nace lo que hoy se le conoce como Internet. Hasta ese entonces ya eran más de 500 nodos conectados a la red. En la época de los años ochenta empieza el crecimiento explosivo de las computadoras personales, esto permitió que muchas compañías se unieran a Internet por primera vez. De esta forma Internet empezó a penetrar en el entorno corporativo apoyando la comunicación en las empresas con sus clientes y proveedores. - Keneth Thompson, el creador de UNIX, demuestra públicamente cómo desarrollar un virus informático. Algo similar realiza un año después el Dr. Fred Cohen en un discurso de agradecimiento con motivo de un homenaje. - Seis años después de la primera demostración, los protocolos TCP/IP son los únicos aprobados por ARPANET. Internet pasa a ser “una serie de redes conectadas entre sí, especialmente las que utilizan el protocolo TCP/IP”.
1985	La primera PC Multimedia	Aunque nace para compartir y suceder a la consola de juegos Atari, la Amiga 1000, creada por Commodore, se convierte en la primera computadora personal “PC” multimedia de gran éxito comercial.
1988	¡Todos a Chatear!	 Jarkko Oikarinen desarrolla el “IRC” (Internet Realy Chat), un programa que permite charlar “en vivo en Internet”
		- Tim Berners-Lee, investigador del CERN (Organización Europea para la Investigación Nuclear) en Suiza, estaba

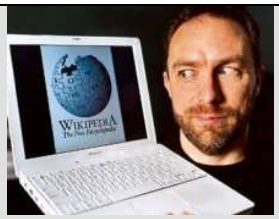
1989	Arpanet le da el paso al Internet comercial	desarrollando un sistema de hipertexto, que permitía "navegar" entre documentos por medio de *hiperligas* de texto e imágenes, con sólo el *click* de un ratón. - Un par de años después aparece el primer navegador gráfico (*browser*) comercial de Internet, el mosaic. Desarrollado por Marc Andreesen y un grupo de estudiantes programadores en la NCSA (National Center for Supercomputing Applications) localizado en la Universidad de Illinois en Urbana Champaign. Internet abrió sus puertas a actividades de tipo comercial y esto ocasionó que nuevos países tuvieran conexión a Internet.
1990	El primer buscador	Buscar y encontrar algo en Internet ya es un problema. La universidad de McGill ofrece el buscador Archie. Al año siguiente llega Wais y Gopher. (Los tres sistemas son anteriores a la www).
1991	El texto se vuelve hipertexto Internet se presenta en sociedad Llega Linux	 	- Tim Berners-Lee mejora la implementación del hipertexto liberándolo al uso público. Mediante el hipertexto el usuario puede saltar de un texto a otro relacionado. La forma más habitual de hipertexto en documentos es la de hipervínculos o referencias cruzadas automáticas que van a otros documentos. El hipertexto no está limitado a datos textuales, también puede asociar dibujos, sonidos o videos. - Vinton Cerf, también conocido como el padre de Internet, crea la Internet Society (ISOC) de la que será presidente entre 1992 y 1995. ISOC es una asociación no gubernamental sin fines de lucro, dedicada exclusivamente al desarrollo mundial de Internet. - Cuando el finlandés Linus Torvalds era estudiante de ingeniería de la Universidad de Helsinki crea el nuevo sistema

		operativo libre.
1993	WWW Comienza el Control Mosaic, primer gran navegador gráfico	- Nace lo que hoy conocemos como WWW (world wide web). - La distribución de las direcciones y la administración de las bases de datos constituyen una dificultad creciente. Para administrar la tarea, se crea la InterNIC (Internet Network Information Center). - Desplazando al Gopher, basado en textos, Mosaic consigue alcanzar gran popularidad: la www se convierte en el acceso preferido a Internet.
1994	Ahora se llama autopista Primer spam Primer buscador basado en textos	- En una conferencia celebrada en la Universidad de los Ángeles, Al Gore acuña la expresión "autopista de la información" para referirse a lo que las computadoras harán en el futuro. Sin embargo se queda corto. - La firma de abogados Canter and Siegel aprovecha Usenet para publicar un aviso de sus servicios legales. Inicia así el spam o correo basura: mensajes no solicitados, habitualmente publicitarios, enviados masivamente. Como su mismo nombre indica, resultan muy molestos para el consumidor. - WebCrawler es creado para rastrear textos y no sólo títulos de páginas web. Con un mecanismo muy similar, otro buscador denominado Lycos se convierte en el primero en obtener éxito comercial.
1995	Incrementa el número de países con conexión Netscape, primer navegador comercial	- El número de países con conexión tuvo un incremento considerable, de 121 a 165 países.  - La compañía Netscape Communications, creado por Marc Andreessen, uno de los creadores de Mosaic, lanza el navegador Netscape. - Dos estudiantes de ingeniería de la Universidad de Stanford, Jerry Yang y David Filo, dedican

	Yahoo!		muchas horas a la creación de listas de sus sitios preferidos. Los dividen en categorías, subcategorías. Casi sin querer, idean el buscador más exitoso de los primeros tiempos de Internet: Yahoo ("Yet Another Hierarchical Officious Oracle"). Aunque sus autores suelen ofrecer una explicación más sencilla, Yahoo se traduce familiarmente como "tonto" o "torpe".
	Amazon vende su primer libro		- La librería virtual Amazon, creada por Jeff Bezos, vende su primer libro. En tan sólo un mes, ya realiza envíos a 45 países. Dos años después, recibe 50,000 visitas diarias. El comercio electrónico ya tiene a uno de sus grandes líderes.
	El primer Internet Explorer		- Microsoft adquiere el código fuente de Mosaic y lanza su navegador oficial del sistema operativo Windows, en el que viene incluido. Las primeras versiones del Explorer no afectan al líder Netscape.
	Remates por la red		- En San José California, Pierre Omidyar funda eBay con la intención de completar una colección de caramelos. Advierte que puede utiliza el sitio para que otras personas ofrezcan lo que ya no usan. Un puntero láser inservible es el primer artículo vendido. Su precio fue de U$S 14.83.
	Llega Altavista		- Se lanza Altavista, un poderoso motor de búsqueda.

1996	El ciberespacio se independiza		- John Perry Barlow, poeta y antiguo letrista del grupo musical Grateful Dead, publica la Declaración de Independencia del Ciberespacio.
	Hotmail	msn Hotmail	- Este primer servicio de e-mail basado en la web, más tarde pasará a pertenecer a Microsoft.
	Inician una segunda Internet.		- 34 universidades de EE.UU. se reúnen para definir los objetivos de Internet2: una red de alta velocidad, centrada en la comunicación académica que se mantiene al margen de la Internet "comercial". Diez años después la red está formada por 200 universidades y medio centenar de empresas de tecnología.
1997	La guerra de los navegadores		- La fiesta de lanzamiento de la nueva versión 4.0 del Internet Explorer celebrada en San Francisco, se convierte en el momento más visible de la denominada Guerra de los Navegadores. Las potencias en conflicto son Explorer y Netscape. Ante el gigantesco logo de su rival, los empleados de Nescape se concentraron exhibiendo un cartel con la leyenda "Netscape 72, Microsoft 18", aludiendo a sus respectivas porciones de mercado.
	Bienvenido, blog		- En su sitio llamado Robot Wisdom, Jorn Barrer decide agrupar y publicar diariamente las cosas más interesantes que encuentra en la red. Aunque ya existían cosas parecidas, Barrer es el primero en denominarlo Weblog ("log" significa "diario"). Otros lo abreviarán "blog". Blog es un sitio web periódicamente actualizado, que recopila cronológicamente textos o artículos de uno o varios autores, apareciendo primero el más reciente. Existen programas especiales para crearlos. El autor siempre conserva la libertad de mantener publicado lo que pretende.

1998	Google		Larry y Sergey Brin fundan Google Inc., la empresa creadora del mayor motor de búsqueda de Internet, en funciones desde apenas un par de años antes. El nombre proviene del término matemático Googol (un 1 seguido de 100 ceros), simboliza la inmensidad de datos que se pueden encontrar en la red.
1999	Abre sus puertas el primer banco virtual	- El First Internet Bank of Indiana ofrece todos los servicios bancarios exclusivamente por la red. Otras entidades se sumarán más adelante.	
	Ataca Melissa	- Cien mil ordenadores se ven atacados por un nuevo y temible virus llamado Melissa. Se colapsan los servicios de email y las casillas de correo se abarrotan de enlaces a sitios pornográficos.	
	Napster se hace escuchar	- Shawn Fanning, un estudiante recién ingresado en una universidad de Boston, envía a 30 amigos un programa creado por él mismo para compartir archivos musicales. En pocos días, diez mil jóvenes lo han bajado. El programa fue objeto de enormes controversias y juicios en relación con los derechos de autor y de las productoras discográficas. ¿El nombre del Programa? Napster.	
	Messenger golpea a la puerta	- El programa de mensajería instantánea diseñado por Microsoft para sus sistemas Windows, comienza su extensa carrera. Tres meses después está a punto de ser reciclado por su escaso éxito. Sin embargo, una inesperada avalancha de usuarios lo vuelve a popularizar, desplazando a su famoso predecesor, el ICQ.	
	Blogger	- Una pequeña empresa de San Francisco, Pyra Labs, lanza este sistema de publicación de Blogs. Blogger ayudará fuertemente a popularizar este formato. En el 2003 es adquirido por Google.	
2000	Apocalipsis, no	Desde hace meses se teme que el paso de la cifra 99 a la 00 en los calendarios internos de las computadoras conduzca al caos, al colapso mundial de los datos informáticos. Sin embargo, nada sucede. Las computadoras, Internet y el mundo siguen su curso.	
			Jimbo Wales, con la ayuda de Larry Sanger, inician el proyecto Wikipedia: una enciclopedia libre y políglota basada en la colaboración.

2001	Nace la Wikipedia		Toda persona con acceso a Internet puede modificar la gran mayoría de los artículos. Llegará a convertirse en la enciclopedia más gigantesca de la historia. Para mediados de 2008 supera los diez millones de artículos en más de 250 idiomas. La palabra Wikipedia combina wiki (que significa "rápido" para los hawaianos) con paideia (educación en griego)
2003	El dominio de los niños		- Se crea el dominio ".kids" para denominar a los sitios seguros para los niños.
	Bajar música ya es legal		- Apple Computer presenta Apple iTunes Music Store, que permite bajar legalmente temas musicales pagando 0.99 dólares por cada uno.
	Una segunda vida para todos		- Nace Second Life, un mundo virtual en donde cualquier persona puede residir a través de su avatar o personaje. Esta segunda vida permite hacer todo lo que se da en la vida real, sin las limitaciones de ésta: amar, trabajar, crear objetos artísticos, edificar una casa y hasta ganar Linden Dólares ($L), moneda intercambiable en el mundo físico. La idea, desarrollada por Linden Lab, resulta muy exitosa: decenas de miles de personas se mueven por su Second Life todos los días. Atraídos por el éxito de Second Life, infinidad de empresas establecen negocios y publicidad en esta economía virtual. Algunos países incluso instalan embajadas.

2004	Facebook muestra la cara		- Pensando en sus compañeros de Harvard, el estudiante Mark Zucherberg crea un sitio web de redes sociales. El nombre alude al folleto que reciben los recién ingresados, con fotos de sus compañeros para ayudar a identificarlos. Muy pronto rebasa el marco universitario. En el 2008 cuenta con cerca de 100 millones de usuarios activos. Facebook permite localizar a personas con quienes se ha perdido el contacto y hacer otros amigos para intercambiar mensajes, fotos y compartir un sinnúmero de actividades.
	Tienes un Gmail		- El nuevo servicio de e-mail de Google ofrece una gran capacidad de almacenamiento gratuito: 1 gigabyte.
	La web se hace social		- Se crea el término Web 2.0 para definir el uso de la www que busca aumentar la creatividad, el intercambio de información y la colaboración entre usuarios.
	¿La Segunda Guerra?		- Se publica el Mozilla Firefox. En los primeros 99 días obtiene 25 millones de descargas. De esta manera se da origen a lo que algunos consideran la “Segunda Guerra de los Navegadores” entre el recién llegado, Internet Explorer y otros como Ópera y Safari.
	Se presenta Digg		- Digg es un sitio web especializado en noticias sobre ciencia y tecnología, creado por Kevin rose, Jay Adilson y otros. Su control

			editorial es democrático, ya que depende de los votos de los usuarios. Los aportes se incorporan a la página principal una vez que han recibido una treintena de “diggs”, que para el caso se traduce como votos. Digg es otro de los sitios emblemáticos de la Web 2.0
2005	Nos vemos en YouTube		Chad Hurley, Steve Chen y Jawed Karim fundan un sitio web que permite a los usuarios compartir videos digitales. La facilidad para alojar videos personales de hasta 10 minutos de duración lo hacen extremadamente popular y a veces polémico. 1,650 millones de dólares convierten a YouTube en propiedad de Google en octubre de 2006. Un mes más tarde es considerado “El invento del Año” por la revista Time
2006	Mil cien millones de usuarios	- Las cifras del crecimiento de Internet no paran de sorprender. A esta altura se especula con que para el año 2015 habrá 2 mil millones de usuarios.	
2007	El Iphone		Apple lanza su teléfono celular capaz de conectarse a Internet.

A nivel mundial ocurrieron una serie de acontecimientos relevantes en la historia de la informática y el Internet, paralelo a ese avance, fueron también surgiendo los primeros virus informáticos hasta llegar a ser más sofisticados y siendo difíciles de detectar. Así mismo surge la necesidad de mantener un mayor nivel de seguridad en las organizaciones, derivado del avance tecnológico. Conforme se perfeccionan los dispositivos de comunicación se tiene que ir perfeccionando la seguridad de ésta, manteniendo siempre los

principios fundamentales de la seguridad informática (integridad, confidencialidad y disponibilidad).

Otro punto interesante para este trabajo de investigación es el conocimiento ahora a nivel nacional sobre la manera en la cuál fue surgiendo la tecnología y el Internet, teniendo en cuenta el año, la época, el tipo de gobierno que existía y sobre todo, lo que tuvo que ocurrir en nuestro país para el desarrollo de éstos grandes avances que han beneficiado en gran medida a todas las personas. A continuación se muestra en tabla 2, una breve reseña sobre los acontecimientos más importantes, desde su surgimiento hasta lo que se conoce actualmente.

Tabla. 1.2 Acontecimientos relevantes de la seguridad informática en México

Año	Acontecimiento		Reseña
1986	El ITESM recibía tráfico de la red de BITNET	TECNOLÓGICO DE MONTERREY®	Antes de que el ITESM (Instituto Tecnológico y de Estudios Superiores de Monterrey) se conectara a Internet, este instituto recibía desde 1986 el tráfico de la red de bitnet (Because It's Time NET-work) mediante este mismo enlace a la UTSA. La UNAM (Universidad Nacional Autónoma de México) se conecto a bitnet hasta octubre de 1987.
1989	Llegada de Internet a México La UNAM	UTSA	- El ITESM (Instituto Tecnológico y de Estudios Superiores de Monterrey) se conecta hacia la escuela de medicina de la UTSA (Universidad de Texas en San Antonio). El enlace era mediante una línea privada analógica a 9600 bps (bits por segundo). - El segundo nodo de Internet en México fue la UNAM. Se conectó mediante un enlace vía satélite de 56Kbps (Kilobits por segundo) hacia el NCAR (National Center of Atmosferic Research) de Boulder

	Primer enlace vía satélite		Colorado de EUA. Posteriormente la UNAM y el ITESM son interconectadas mediante el enlace de BITNET. La tercer institución que logró la conexión a Internet fue el ITESM campus Estado de México, también a través de NCAR. - El CICESE (Centro de Investigación Científica y Educación Superior de Ensenada) llevó a cabo el primer enlace vía satélite en México para acceso exclusivo a Internet en el nodo del Centro de Supercomputadoras de San Diego (SDSC, San Diego Supercomputer Center) localizado en la Universidad de California en San Diego (UCSD, University of California in San Diego).
1994	Se fusiona Mexnet y Conyt	Se fusionaron las redes de información electrónica de mexnet y de Conyt a partir de lo cual fue creada la Red de Tecnología Nacional (RTN) con un enlace de 2Mbps (megabits por segundo). Hasta ese entonces el uso de Internet estaba reservado para las instituciones educativas y centros de investigación pero posteriormente se abrió al uso comercial iniciando así la gestión del dominio *.com.mx.*	
1995	Internet entra al uso comercial Crecen los dominios Se Crea NIC-México	- En octubre de ese año el número de dominios *.com* ascendió a 100, rebasando al número de dominios formado por las instituciones educativas. - El crecimiento de los dominios de 1995 a 1996 fue de más de 1000%, pasando de 180 A 2286 nombres de dominio. - Debido al crecimiento en los dominios en noviembre se crea NIC-México (Network Information Center) entidad encargada de administrar y asignar los nombres de los dominios bajo la designación *.mx* y de las direcciones de Internet Protocol.	
			La CUDI es una asociación civil de

1999	Se funda el CUDI (Corporación Universitaria para el Desarrollo de Internet)		carácter privado, sin fines de lucro, integrada por las universidades del país. Su misión es promover y coordinar el desarrollo de una red de telecomunicaciones de la más avanzada tecnología y de alta capacidad, enfocada al desarrollo científico y educativo en México. CUDI es el organismo que maneja el proyecto de la red Internet 2 en México y busca impulsar el desarrollo de aplicaciones que utilicen esta red, fomentando la colaboración en proyectos de investigación y educación entre sus miembros.
	Compran a Datanet e Internet de México		-PSINet, Proveedor estadounidense de Servicios comerciales de Internet toma cobertura como uno de los prestadores principales de servicios relacionados en Latinoamérica por medio de la compra de ISPs locales en México y Brasil.
2000	Crecimiento de Internet	Internet atestigua un gran crecimiento, cientos de proveedores de acceso a Internet (ISPS, Internet Service Providers) que brindan conexiones a Internet a través de diversas tecnologías de acceso.	
2001	Aumento de un 65% de usuarios de Internet en México	- México registró un aumento de un 65% de usuarios de Internet con respecto al año anterior. Asimismo, se informó que cerca de 16,000 compañías habían realizado transacciones online y el segmento que más se desarrolló en el 2000 fue el B2B que actualmente representa el 70% de las transacciones online en ese país.	
	Ofrecen en la red voces sin censura (Cultura)	- Radio a través de Internet a diferencia de las estaciones convencionales, las emisoras que transmiten por el ciberespacio ofrecen mayor libertad temática y bidireccionalidad. Existen más de 300 estaciones de radio por Internet en México. Tan sólo en live365 (www.live365.com), que es uno de los servidores gratuitos más populares, se hospedan 277	

		estaciones independientes que transmiten desde allá.	
2003	Alertan sobre los riesgos de utilizar Internet en México	La Comisión Nacional para la protección y Defensa de los Usuarios de Servicios Financieros (Condusef) alertó sobre los riesgos de utilizar Internet como medio para realizar operaciones financieras. “Hay falta de seguridad en las transacciones a través de la red, lo que pone en clara desventaja a los clientes”	
2005	Crecen 190% clientes De Internet rápido de Telmex	TELMEX	- Precisa la firma que tiene un millón 850 mil cuentas de acceso en México, de las cuales 665 mil 321 son de banda ancha, es decir, poco más del 35%. Teléfonos de México (Telmex) registró en el último año un alza de 190% en su número de clientes de Internet de banda ancha, lo que le llevó a invertir mil 500 millones de dólares en el país en 2004.
	Aumentan 81% compras por Internet en México	AMIPCI Asociación Mexicana de Internet	- Informa la Asociación Mexicana de Internet (AMIPCI) que durante el primer trimestre del 2005 el monto total de las ventas vía electrónica alcanzó 806 millones 450 mil pesos; el sector de viajes es el que presenta mayor crecimiento.
2006	Celebran Día del Internet en México		- La Asociación Mexicana de Internet (AMIPCI) celebrará el Día del Internet (17 de Mayo) para conmemorar 20 años de la primera conexión a la red de México, con lo que se une a la celebración de España, Argentina, Brasil, Chile y Colombia.
	Dixo.com descubre fórmula para negocio en Internet en		- Benavides, productor radiofónico de 27 años y Lambertini, músico e ingeniero de audio de 23 años, trazaron la idea básica de Dixo que era: “si te gusta leer, puedes leer,

	México Avanza el uso de Internet en México: AMIPCI (Asociación Mexicana de Internet)		sino eres de los que lee, te puedes pasar a escuchar, sino puedes verlo en videoblog y de paso te puedes ganar boletos para ir a algún lado". - Según un estudio de AMPICI México terminará el 2006 con 20.2 millones de usuarios de Internet, de los cuales el 58% está constituido por jóvenes entre los 12 y 14 años.
2007	Es lenta la conexión a Internet en México	México es de los países que evolucionan más lentamente en el incremento de la velocidad de las conexiones a Internet y la reducción de las tarifas de banda ancha, según la Organización para la Cooperación y Desarrollo Económicos (OCDE).	
2008	Ciudades digitales y tecnología 3G aceleran uso de Internet en México		Según la Asociación Mexicana de Internet (AMIPCI) sólo 6.20% de los 23.7 millones de usuarios de Internet registrados en 2007 navegan vía celular, PDA o Blackberry. La meta del gobierno federal de alcanzar 70 millones de internautas en 2012 es distante si se considera que en la actualidad la cifra es de más de 23 millones.
2009	Usuarios de Internet en México crecieron en un 341% en últimos ocho años Impulsan evolución de Internet en México	- El número de usuarios de Internet en marzo de este año en México ascendió a 22,3 millones de personas, cifra 341% superior a la registrada en 2000, cuando había 5,05 millones. - Para impulsar el desarrollo de la web 3.0 en México, la siguiente etapa en la evolución de Internet, Infotec lanzó su plataforma SemanticWebBuilder, la cual puede descargarse de manera gratuita y permite crear en un par de minutos sitios web, cuya principal característica será facilitar la búsqueda de información.	

De la tabla 1.2 se aprecia que en nuestro país desde hace aproximadamente 20 años se tiene acceso a Internet y desde hace 10 años entra como uso comercial, lo que implica que en esta última década éste se ha incrementado de manera masiva lo que conlleva a mantener seguros los sistemas de comunicación, de no ser así, se está expuesto a padecer alguna amenaza en los sistemas informáticos.

Después del análisis realizado sobre el desarrollo histórico de la tecnología informática tanto en el mundo como en nuestro país que se puede observar como ha ido evolucionando la comunicación entre los diversos países y el impacto que ha tenido en México, por ejemplo, se aprecian en las tablas 1.1 y 1.2 el momento en el cual surgió el Internet por vez primera y su evolución hasta nuestros días.

Dicha herramienta ha sido de gran utilidad tanto para las organizaciones como para las universidades y la gente en común, por ello es importante aprovechar los recursos con los que se cuenta hoy en día y así ayudar al desarrollo de nuestro país.

1.4 Desarrollo de la Seguridad Informática en México y en el Mundo

El desarrollo de la seguridad informática a nivel nacional como internacional ha ido creciendo día con día. Para tener una idea de este desarrollo es conveniente conocer el impacto que ha tenido el Internet a nivel mundial.

En la tabla 1.3 se muestran los principales países con mayor número de usuarios que acceden a Internet, este estudio fue realizado por el Internet World Stats “Estadísticas del mundo en Internet” y se tomaron en cuenta los siguientes aspectos: Lugar que ocupa cada país, Índice de población de cada país respecto al 2008, Número de usuarios que utilizan Internet, Porcentaje de crecimiento en el periodo comprendido del 2000 al 2008 y Porcentaje de usuarios a nivel mundial.

Tabla 1.3. Países con el mayor número de usuarios de Internet

Países con el mayor número de usuarios de Internet						
#	País o Region	Población 2010	Usuarios Datos Recientes	% Población	Crecimiento 2000-2010	% Usuarios Mundo
1	China	1,330,141,295	420,000,000	31.6%	1,766.7%	21.4%
2	Estados Unidos	310,232,863	239,893,600	77.3%	151.6%	12.2%
3	Japón	126,804,433	99,143,700	78.2%	110.6%	5.0%
4	India	1,173,108,018	81,000,000	69.0%	1,520.0%	4.1%
5	Brasil	201,103,330	75,943,600	37.8%	14,18.9%	3.9%
6	Alemania	82,282,988	65,123,800	79.1%	171.3%	3.3%
7	Russia	139,390,205	59,700,000	42.8%	1,825.8%	3.0%
8	Reino Unido	62,348,447	51,442,100	82.5%	234.0%	2.6%
9	Francia	64,768,389	44,625,300	68.9%	425.0%	2.3%
10	Nigeria	152,217,341	43,982,200	28.9%	21,891.1%	2.2%
11	Corea del Sur	48,636,068	39,440,000	81.1%	107.1%	2.0%
12	Turquía	77,804,122	35,000,000	45.0%	1,650.0%	1.8%
13	Iran	76,923,300	33,200,000	43.2%	13,180.0%	1.7%
14	**México**	**112,468,855**	**30,600,000**	**27.2%**	**10,28.2%**	**1.6%**
15	Italia	58,090,681	30,026,400	51.7%	127.5%	1.5%
16	Indonesia	242,968,342	30,000,000	12.3%	1,400.0%	1.5%
17	Filipinas	99,900,177	29,700,000	29.7%	1,385.0%	1.5%
18	España	46,505,963	29,093,984	62.6%	440.0%	1.5%
19	Argentina	41,343,201	26,614,813	64.4%	964.6%	1.4%
20	Canadá	33,759,742	26,224,900	77.7%	106.5%	1.3%
20 Países		4,480,797,760	1,490,754,397	33.3%	417.8%	75.8%
Resto del Mundo		2,364,812,200	475,760,419	20.1%	551.2%	24.2%
Total Mundial Usuarios		6,845,609,960	1,966,514,816	28.7%	444.8%	100.00%

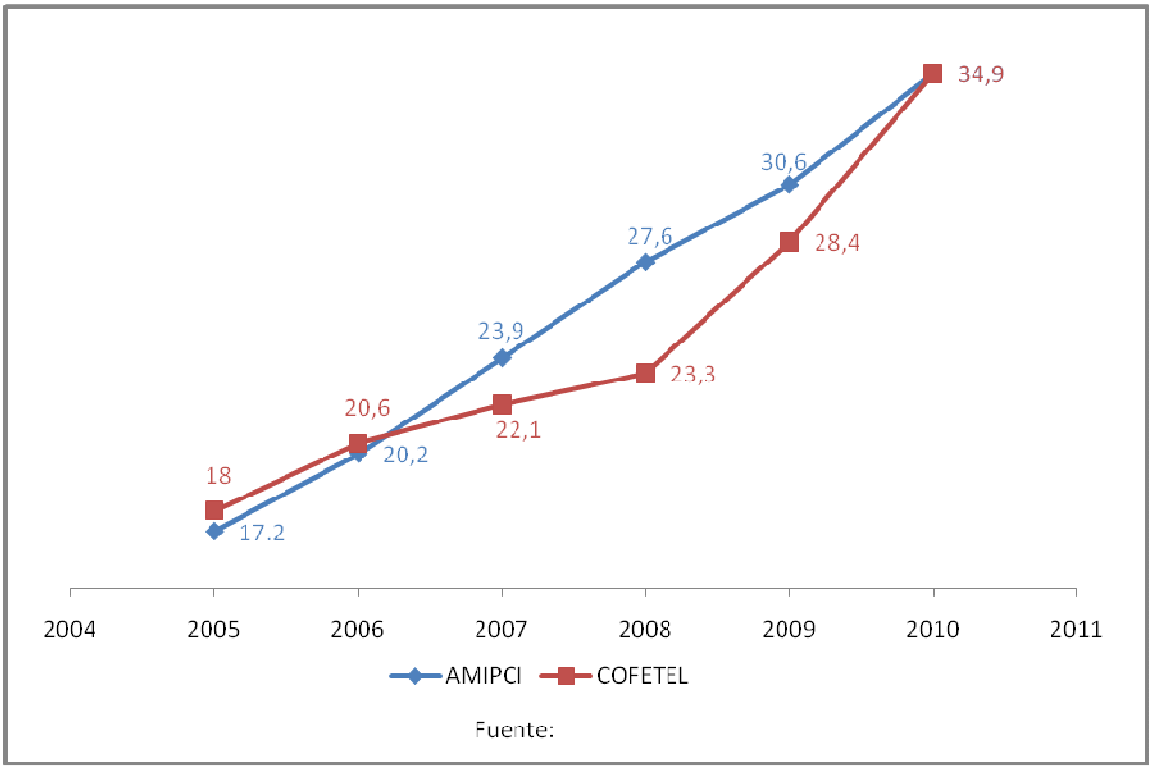
NOTES: (1) World Internet User Statistics were updated for June 30, 2009. (2) Additional data for individual countries and regions may be found by clicking each country name. (3) The most recent user information comes from data published by Nielsen Online, International Telecommunications Union, Official country reports, and other trustworthy research sources. (6) Data from this site may be cited, giving due credit and establishing an active link back to Internet World Stats. Copyright © 2001 - 2009, Miniwatts Marketing Group. All rights reserved.[11]

Como se puede apreciar en la tabla 1.3, México ocupa el catorceavo lugar considerando que cuenta con una población de 112, 468,855 personas, de las cuales el 27.2% son usuarios que tienen acceso a Internet lo que equivale a nivel mundial al 1.6%. El primer lugar con respecto al mundo lo ocupa China con el 21.4% de usuarios que acceden a Internet seguido de Estados Unidos con el 12.2% y Japón con el 5.0% y el último lugar lo ocupa Canadá con

[11] http://www.internetworldstats.com/top20.htm

el 1.3%. Estos 20 países representan el 75.8% de usuarios que utilizan Internet con respecto al resto de los países del mundo que representan el 24.2%.

Con lo que respecta a nuestro país, existe un estudio realizado por la Asociación Mexicana de Internet (AMIPCI) sobre los hábitos de los Internautas en México realizado en Mayo de 2011. Este estudio analiza los principales hábitos de los internautas en nuestro país, así como el impacto que han tenido las redes sociales. Los datos estadísticos que muestra este informe provienen de distintas fuentes como: CONAPO (Consejo Nacional de Población), INEGI (Instituto Nacional de Estadística y Geografía), COFETEL (Comisión Federal de Telecomunicaciones) y del Departamento de Investigación Online de la empresa ELOGIA. En la gráfica 1.1 se muestra el histórico de usuarios de Internet en México con respecto al año 2005 – 2010.



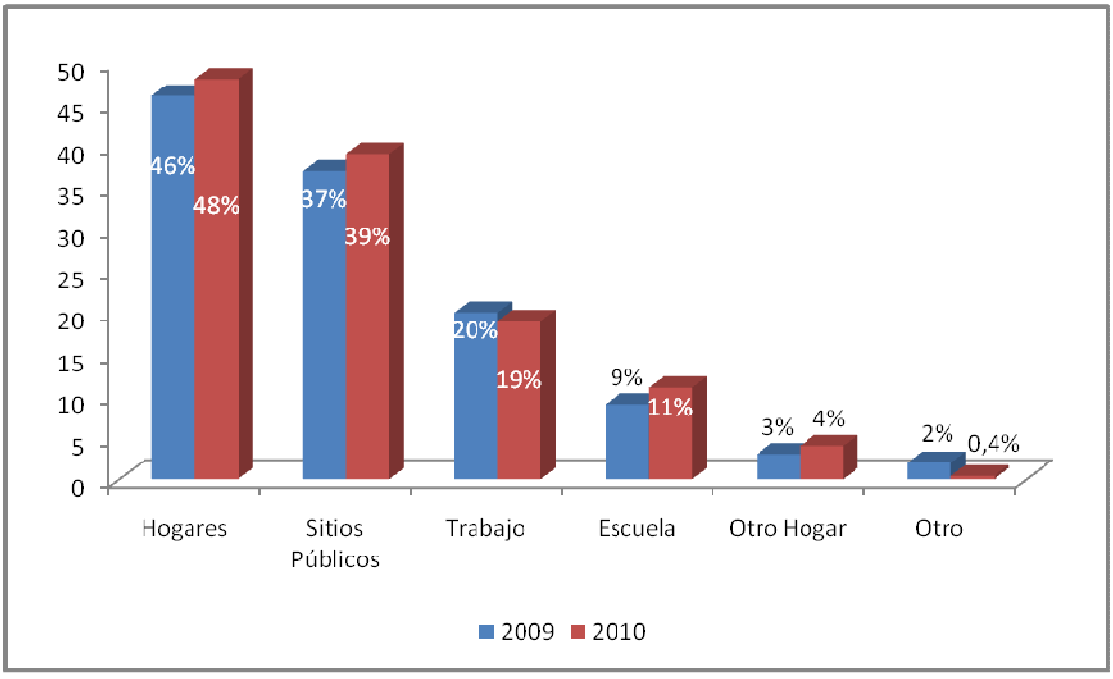
Gráfica 1.1 Histórico de usuarios de Internet en México 2005 – 2010 (Cifras en Millones)

Se aprecia que en el año 2005 habían aproximadamente 18 millones de internautas, según datos proporcionados de la COFETEL, en ese mismo año AMIPCI registró 17.2 millones

de internautas. Con el paso de los años estas cifras han ido aumentando considerablemente llegando al año 2010 a 34.9 millones de internautas.

De todos los 34.9 millones de usuarios que tienen acceso a Internet el 51% son hombres y el 49% son mujeres, lo que implica que ambos géneros están prácticamente en circunstancias iguales y por ello es necesario que desde la educación básica se les enseñe a los alumnos a utilizar los equipos de comunicación de manera eficiente, para que naveguen de manera segura.

En la gráfica 1.2 se muestran los lugares más comunes donde navegan los internautas con respecto a los años 2009 y 2010. Se aprecia que el hogar, sigue siendo el principal lugar en donde los usuarios utilizan Internet, seguido de los sitios públicos, el trabajo, la escuela, entre otros.



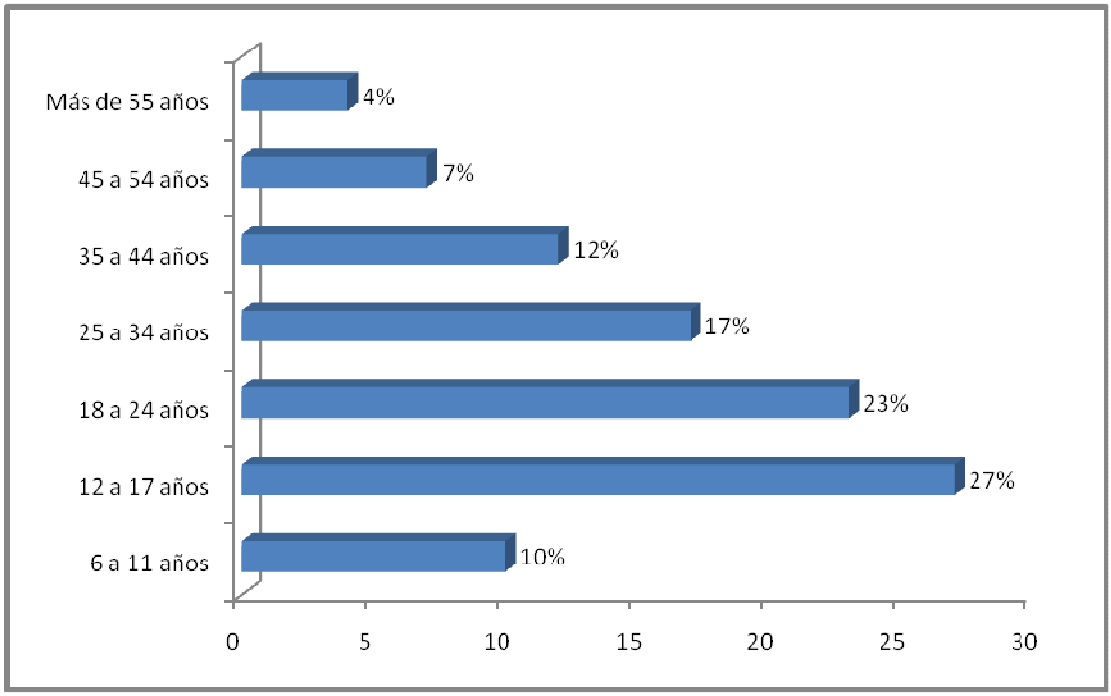
Gráfica 1.2 Usuarios de Internet por lugar de acceso 2000-2010

Las variaciones con respecto al año 2009 y 2010 son bajas, ya que incluso en el hogar se ha aumentado este porcentaje. En donde disminuyó muy poco es en el lugar de trabajo con un 1%. Un dato importante que se muestra en la gráfica es que en las escuelas hubo un

aumento del 2% en el año 2010 con respecto al 2009, lo que implica que cada vez, son más los alumnos que tienen la posibilidad de acceder a Internet.

Por ello es conveniente que los usuarios conozcan a lo que están expuestos si no navegan de una manera clara y confiable, ya que de lo contrario serán víctimas de cualquier tipo de amenaza, según la situación que se presente.

En la siguiente gráfica 1.3 se muestra una distribución de usuarios de internet por edad durante el año 2010.

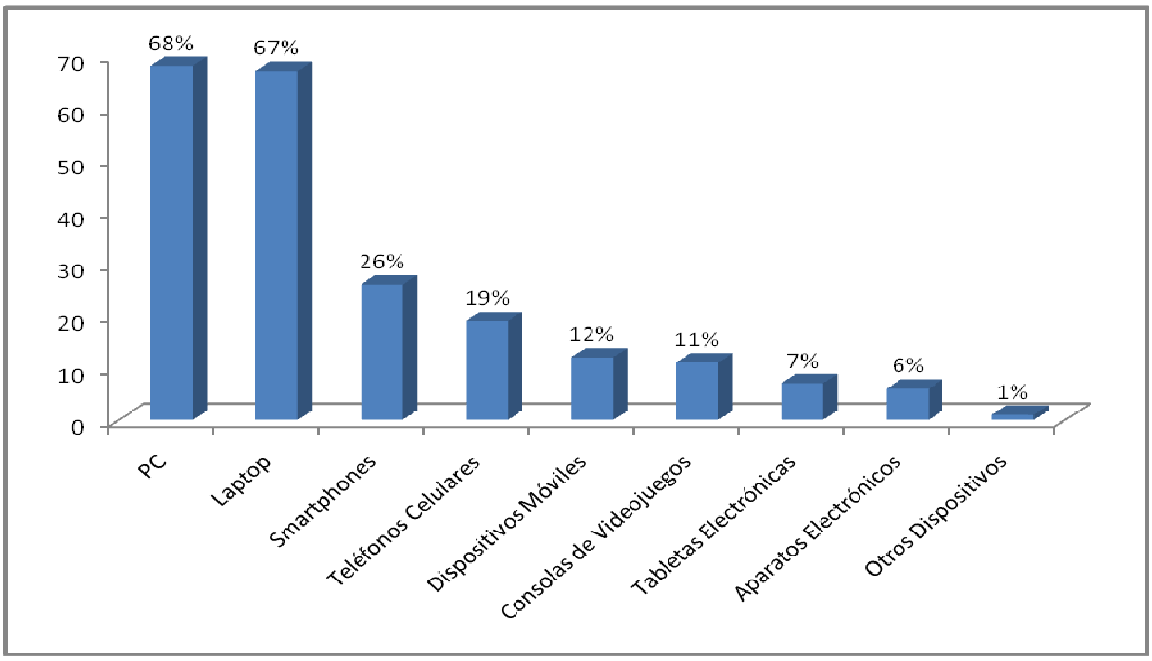


Gráfica 1.3 Distribución de Usuarios de Internet por Grupos de Edad, 2010

Se observa que los usuarios que más navegan tienen entre 12 y 17 años, ocupando el 27%, seguido de los de 18 a 24 años con un 23% y en último lugar lo ocupan las personas mayores de 55 años con el 4%.

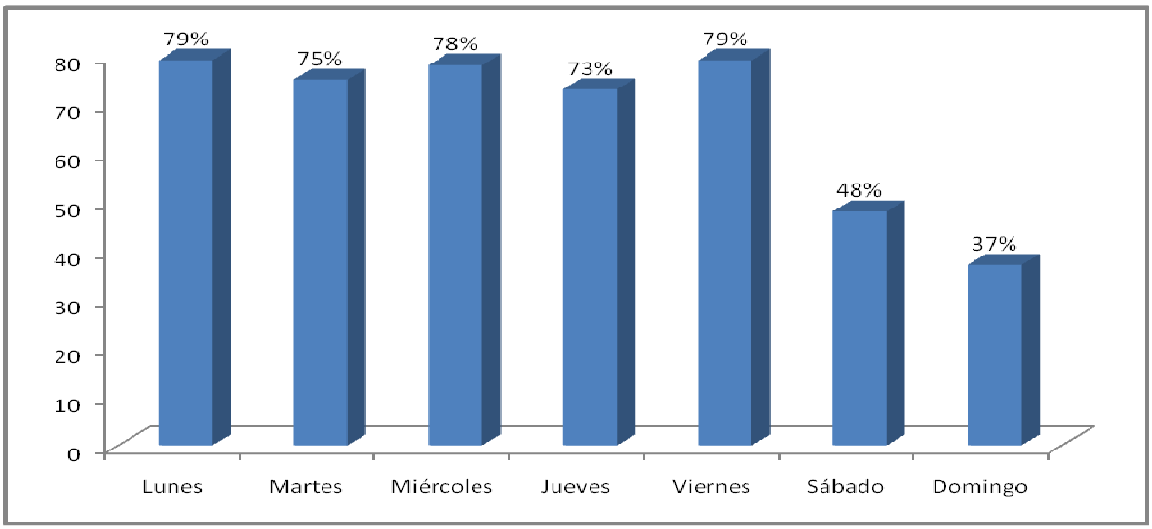
En la gráfica 1.4 se muestran los dispositivos utilizados para conectarse a Internet y en primer lugar se encuentra la PC con un 68%, seguido de las Laptop con un 67%, en tercer lugar los smartphones con un 27%, lo que implica que cada vez son más los usuarios que

cuentan con este tipo de dispositivos debido a la expansión de los puntos de acceso de redes inalámbricas. En menor grado le siguen los celulares, dispositivos móviles, consolas, tabletas y aparatos electrónicos.



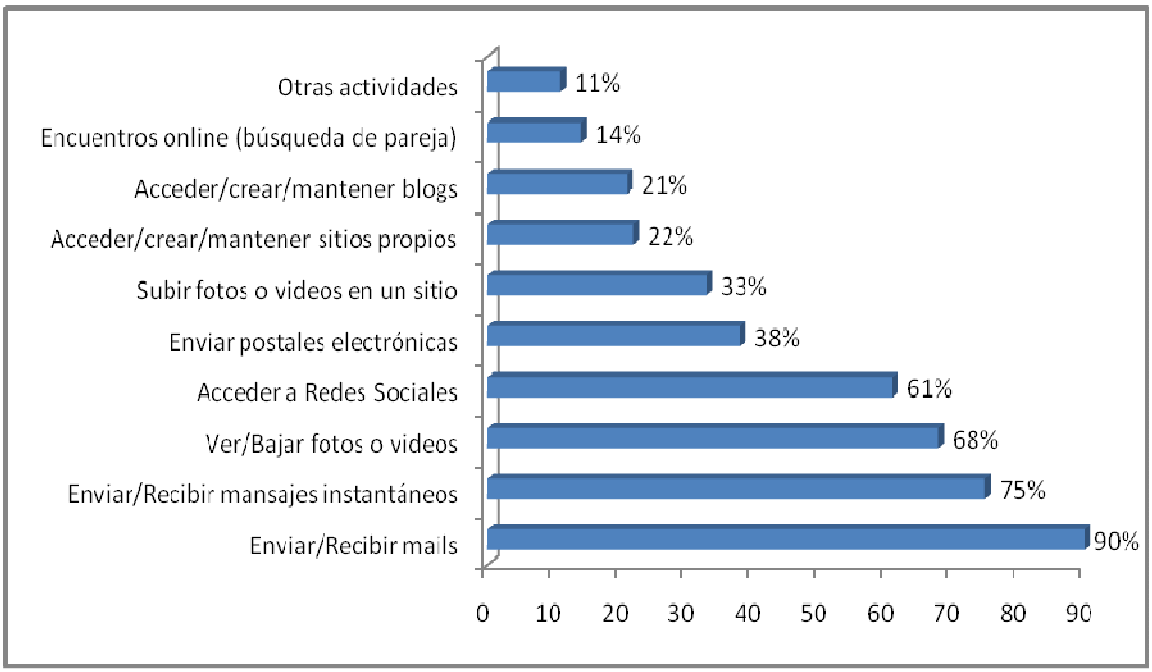
Gráfica 1.4 Dispositivos usados por el Internauta Mexicano para conectarse a Internet

En la gráfica 1.5 se muestran los días de la semana en que los usuarios se conectan a Internet, y se aprecia que la mayor actividad del Internauta Mexicano es de lunes a viernes.



Gráfica 1.5 Conexión por día de la semana

Un dato interesante que se dio a conocer en este informe es que durante el 2010 el tiempo promedio de conexión del Internauta Mexicano fue de 3 horas y 32 minutos, 11 minutos más que en el 2009 y las principales actividades sociales online que realizan los internautas Mexicanos son los que se muestran en la gráfica 1.6.

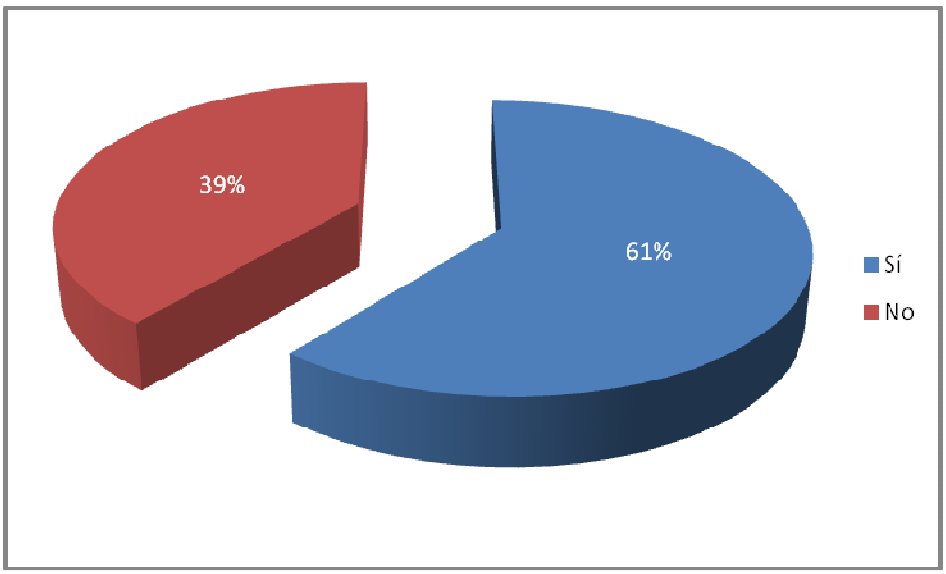


Gráfica 1.6 Principales Actividades Sociales Online

Se aprecia que en primer lugar aparece el correo electrónico como actividad principal con el 90%, seguido de los mensajes instantáneos con el 75%, así como ver o bajar fotos y videos con el 68% y en cuarto lugar se encuentran las redes sociales con el 61%.

Por otra parte, las principales actividades de entretenimiento online ahora son las redes sociales, ya que según AMIPCI 8 de cada 10 entrevistados contacta amigos y conocidos por medio de las redes sociales.

En la gráfica 1.7 se aprecia que el 61% utiliza las redes sociales y el 39% no. A lo que se concluye que 6 de cada 10 mexicanos acceden a alguna red social.



Gráfica 1.7 Uso de redes sociales

Según AMIPCI por distribución de género son 5% más las Mujeres que Hombres que acceden a alguna red social.

Por lo tanto se concluye que en el 2010 el número de internautas alcanzó los 34.9 millones, por otro lado, el servicio de internet en los hogares tiene una mayor penetración en ciudades de más de 100,000 habitantes por lo que es importante trabajar en materia de seguridad informática basándose en los diversos niveles educativos para que los jóvenes conozcan la importancia de mantener los equipos de comunicación seguros e incluso que tengan las herramientas para evitar ser víctimas de cualquier usuario mal intencionado.

1.5 Importancia de la Seguridad Informática

La *seguridad informática* está presente en todas las áreas por ejemplo: ingeniería, industria, administraciones públicas, medicina, diseño, arquitectura, investigación y desarrollo, administración de empresas, restauración y arte, etc., es por ello que se debe de tener en cuenta el hecho de concientizar al personal que labora en las diferentes organizaciones para proteger la información, que es el activo más importante de toda organización.

La seguridad informática se ha convertido en un factor sumamente importante principalmente para las organizaciones a nivel mundial ya que se tenía la creencia de que muy difícilmente les puede ocurrir alguna tragedia, pero hay acontecimientos que han perjudicado a las empresas como fue el caso de los Estados Unidos el 11 de septiembre del 2001, el centro financiero de Nueva York sufrió uno de los atentados más impactantes que se hayan vivido, fallecieron más de dos mil personas, también desapareció valiosísima información de las empresas. Por esta razón a partir de ese acontecimiento, compañías de todas partes del mundo comenzaron a tomar conciencia de la importancia de resguardar los datos y de contar con un DataCenter (Centro de Datos) que es aquella ubicación física en donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. Así como se muestra en la siguiente figura 1.1

Figura 1.1 Datacenter o Centro de Cómputo

Las compañías fueron entendiendo que no solo se trataba de mantener la seguridad a nivel de datos, sino que ésta debía de extenderse hacia toda la infraestructura que rodeaba la información para asegurar la continuidad del negocio, invirtiendo más en los diferentes aspectos en cuanto a seguridad se refiere como por ejemplo; seguridad física, lógica y sobre todo del personal.

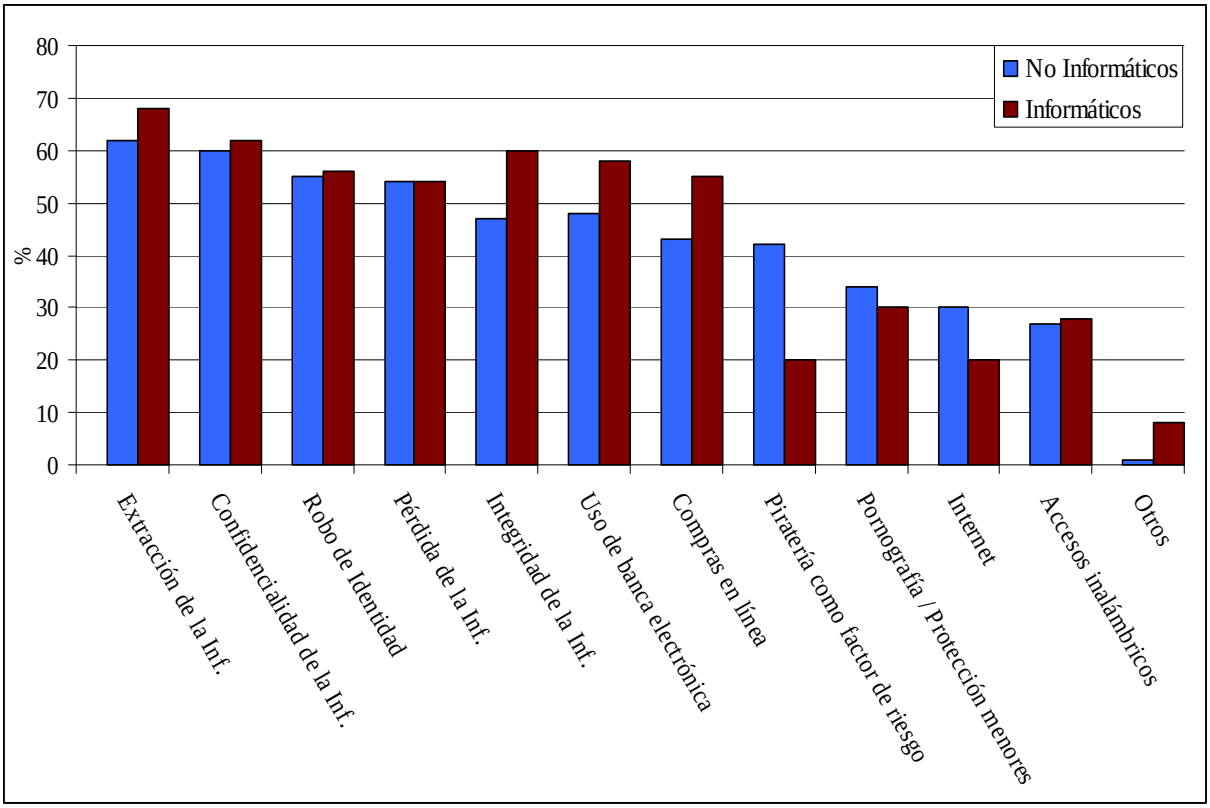
Independientemente de las catástrofes que pudieran atentar contra la integridad de la información de las empresas, éstas comenzaron a tomar conciencia de la necesidad de las auditorías y procesos de aseguramiento del servicio como por ejemplo las leyes Sarbane-Oxley (también conocida como ley SOx) esta ley nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en la bolsa, evitando que las acciones de las mismas, sean alteradas de manera dudosa. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor. Estas leyes son exigidas para todas las empresas que cotizan en la bolsa de los Estados Unidos y se han transformado en una tendencia mundial, impulsando a las compañías a cumplir estándares mínimos, los cuales las llevan a contratar servicios de DataCenters, de lo contrario se producen brechas de seguridad indeseables para sus propios clientes que contratan sus servicios o compran sus productos. Todo esto se ha transformado en una problemática cultural para las empresas, ya que deben de tomar conciencia que la pérdida de datos significa problemas legales y de supervivencia.

En nuestro país se llevó a cabo un estudio de Percepción sobre seguridad informática en el 2008 realizado por la empresa Joint Future Systems, S.C.[12] la cual, considera que el avance en cuanto a concientizar a las empresas sobre la importancia de la seguridad informática aún es muy lento.

El estudio señala que el 10% de todos los entrevistados mostró conocer alguna norma, regulación o estándar (ISO 9000/9001, Sarbanex-Oxley, ISO/IEC, ITIL, ISO 27001, ISO 17799, COBIT, BS 270001, IEEE, SISA y SSL) relacionado con la Seguridad Informática, por lo tanto, el marco regulatorio y legal, sigue siendo percibido por los especialistas como el mayor problema para el país.

[12] http://www.slideshare.net/mariourena/jfs-estudio-de-percepcion-en-seguridad-de-la-informacin-2011-epsim

En la gráfica 1.5 se muestran las principales preocupaciones tanto de los usuarios Informáticos (personal relacionado con la informática) y de los usuarios No-Informáticos (personal No dedicado a la informática)

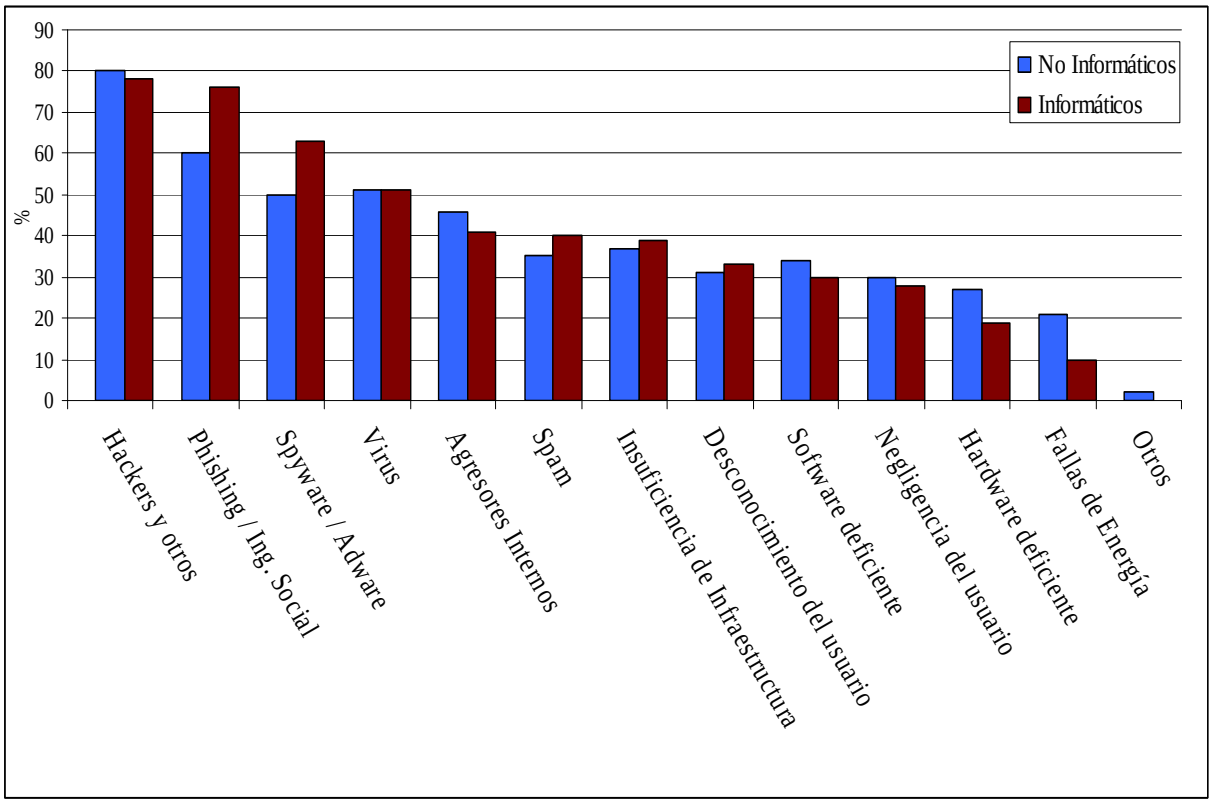


Gráfica 1.8 Principales preocupaciones de los usuarios

Por lo tanto se observa que las principales preocupaciones de los usuarios acerca de la seguridad de los equipos de cómputo es la extracción de la información la cual fue considerada como la principal, seguida de la confidencialidad de la información y robo de ésta. Mientras que en el 2007 sobresalieron otros conceptos como la Pérdida de información y la Invasión a la Privacidad. La menor preocupación que se dio a conocer son el internet y los accesos inalámbricos.

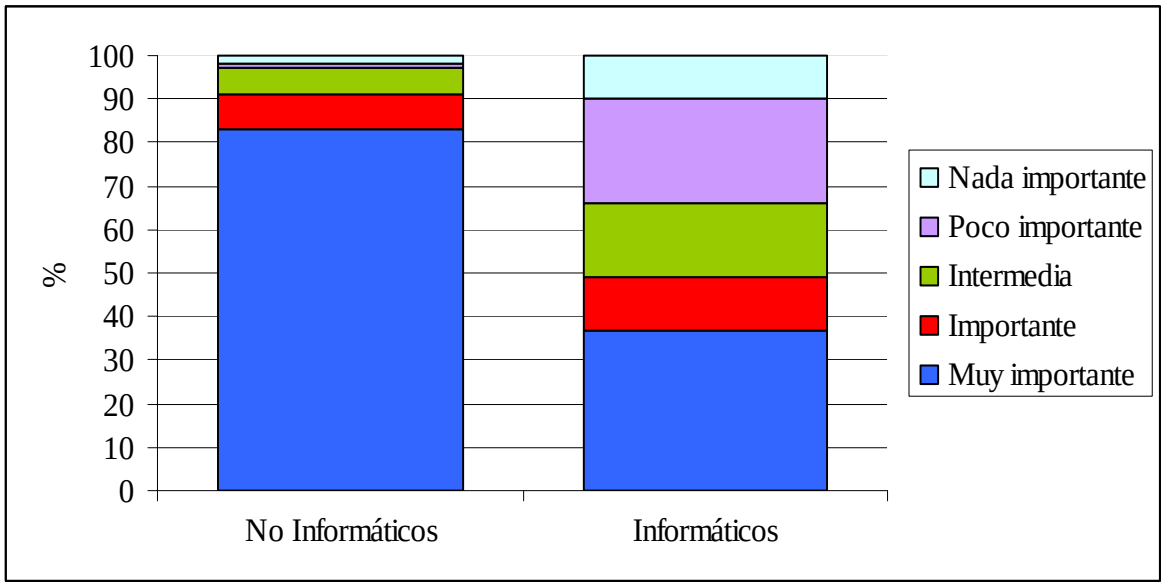
En la gráfica 1.6 se muestran las amenazas identificadas con mayor riesgo. Los usuarios perciben que el atacante más que ocasionar un daño por el gusto de hacerlo, busca obtener algún beneficio adicional, principalmente económico.

Se puede observar que las amenazas con mayor número de menciones para los Informáticos fueron los Hackers y otros agresores externos con un 78.88%, así como el phishing/Ingeniería social con un 75%, seguido del Spyware/Adware con un 65%. Finalmente en menor grado se encuentran el hardware deficiente, representando el 19% y las fallas a la energía eléctrica con un 10%.



Gráfica 1.9 Amenazas percibidas de mayor riesgo

En la gráfica 1.7 se puede apreciar que el 82.9% de los No-Informáticos percibe que la Seguridad en Informática es muy importante para los directivos de la empresa donde trabajan, únicamente el 34.73% de los Informáticos lo percibe de la misma manera, lo que implica que se debe de trabajar arduamente para concientizar a los usuarios que utilizan un sistema de cómputo y así evitar posibles amenazas a los sistemas de comunicación.



Gráfica 1.10 Importancia de la seguridad informática

Por lo tanto se puede decir, que los aspectos más relevantes en este estudio fueron los siguientes:

Principales rezagos en el país:

- Existen huecos legales y de normatividad.
- No se ha logrado difundir una cultura de seguridad entre los usuarios de tecnología ni se tiene una actitud proactiva a nivel organizacional.
- México no ha logrado ser un país productor de soluciones tecnológicas. Aún son muy escasos el desarrollo y la investigación.
- La dirección de la mayoría de las empresas, no ha identificado a la Seguridad en Informática como una actividad estratégica del negocio.

Principales Avances en el País:

- Cada vez más se cuenta con personas capacitadas en primer orden, en el país.
- La figura del Oficial de Seguridad empieza a ser cada vez más frecuente, al menos en organizaciones grandes.
- Los grandes corporativos y el gobierno, empiezan a ser más conscientes de la importancia de contar con programas específicos de Seguridad en Informática y de promover buenas prácticas al interior de sus organizaciones.

Día con día la seguridad informática ha ido adquiriendo mayor importancia, derivado del avance tecnológico que existe en todo el mundo. Estos avances han dado muchos beneficios a las organizaciones pero al mismo tiempo se han presentado diversos problemas que hoy en día se conocen como Ataques Cibernéticos, para entender en donde se está situado, es recomendable definir el concepto de "Ataque Cibernético". El diccionario de la real academia de la lengua define la palabra ataque como: "causar daño" y por cibernético a la "Ciencia que estudia la construcción de sistemas electrónicos y mecánicos a partir de su comparación con los sistemas de comunicación y regulación automática de los seres vivos". Por lo tanto se puede decir que un Ataque Cibernético es la acción de causar un daño a los sistemas electrónicos.

Por lo antes definido es necesario proteger los sistemas de comunicación manteniendo un nivel de seguridad adecuado de acuerdo con las necesidades de cada organización ya que la mayoría de éstas hoy en día siguen experimentando problemas en sus sistemas y en casos extremos debido a la falta de seguridad terminan en bancarrota.
La mayoría de las organizaciones se cuestionan sobre ¿qué deben hacer? o ¿Porqué siguen teniendo problemas? o ¿Por qué deberían de invertir en seguridad si no les ha sucedido nada?

Para responder a las preguntas anteriores es conveniente identificar los aspectos más importantes en una organización que es la Información, teniendo en cuenta que el objetivo de la seguridad informática es mantener la Integridad, Disponibilidad, Confidencialidad de la información, por ello se recomienda pensar en lo siguiente:

- ¿Qué puede ocurrir si no se protege la información?
    - Cualquier persona puede hacer un uso indebido de ésta provocando grandes daños.
    - Se está expuesto a tener diversos tipos de ataques, por ejemplo:
        - Impacto Tecnológico.
        - Impacto económico, laboral y/o financiero.
        - Impacto legal, laboral y/o político.

- ¿Si ocurriera, qué tan malo sería?

El peor panorama que puede ocurrir es que las aplicaciones que no tienen un nivel de seguridad adecuado, sufran de una pérdida total o parcial de la información generando consecuencias como:

- Pérdida de Beneficios.
- Daños en la Reputación (Calidad).
- Interrupción de los Procesos de Negocios.
- Bajo Incremento en la Productividad de la Empresa.
- Consecuencias Legales.
- Deterioro en la Confianza de los Clientes.
- Pérdida de Empleos.

- ¿Cómo se puede proteger?
    - Herramientas de seguridad.
    - Políticas de Seguridad.
    - Capacitación.

Como se puede apreciar, se dan algunas sugerencias al responderse a cada una de las preguntas, con la finalidad de que las organizaciones puedan crear planes de seguridad a fin de estar prevenidos ante cualquier evento.

1.6 Situación Actual de México con respecto al exterior

En México aún falta mucho por hacer en cuanto a seguridad informática, ya que depende de varios factores, principalmente gubernamentales. Es un hecho que se ha tenido un avance si se hace una comparación con países como Turquía, Argentina, Polonia, etc. pero simplemente con el país vecino Estados Unidos o con Japón aún estamos muy lejos de estar al nivel de ellos. En la tabla 1.4 se muestran algunos acontecimientos tecnológicos que presenta México a lo largo del año 2009.

Tabla 1.4 Situación actual de México con respecto al exterior

Acontecimiento de la SI	Resumen
El DF es la segunda ciudad con más ataques cibernéticos en AL	La ciudad de México es la segunda urbe de América Latina que más ataques cibernéticos recibe sólo por detrás de Buenos Aires, esto según el Informe Mundial sobre Amenazas a la Seguridad en Internet de la empresa Symantec realizado el primer semestre de 2006.
Hackeo de cajeros, una moda tecnológica	En México y América Latina, los fraudes financieros cometidos por Internet han aumentado cerca del 50 por ciento desde que estalló la crisis económica a finales del año pasado.
México ocupa tercer lugar mundial en ciber-ataques	Actualmente nuestro país pasó del cuarto al tercer lugar en recibir ataques cibernéticos, según Symantec.
Crece la banda ancha, pese a todo	Un estudio de The Competitive Intelligen- ce Unit señala que, a pesar de la ausencia de una política pública integral y de alto impacto para promover al acceso universal de los mexicanos a servicios de banda ancha, el mercado ha logrado, incrementar el número de accesos en nuestro país. Señala que las suscripciones a Internet de banda ancha crecieron 50% entre 2007 y 2008.
Alertan software de seguridad falso	El software de seguridad falso es una de las principales amenazas para la seguridad informática en todo el mundo, según el último informe de seguridad elaborado por el grupo Microsoft quien detectó dos familias de software de seguridad falso, FakeXPA y FakeSecSenwere, en más de 1.5 millones de computadoras de todo el mundo, lo que las sitúa entre las diez amenazas más graves en el segundo semestre de 2008. El Reporte de Inteligencia de Seguridad de Microsoft incluye menciones específicas sobre México y Brasil, dos países especialmente afectados por el software dañino. España aparece también como uno de los 25 países con

	mayor tasa de computadores infectados en el segundo semestre de 2008, con un promedio de 19.2 de cada mil computadoras limpiadas.
La CFE llevará fibra óptica a Centroamérica.	La Comisión Federal de Electricidad (CFE) adquirió el 11% de las acciones de Sistema de Interconexión Eléctrica para América Central (SIEPAC) –en la que participan Costa Rica, El Salvador, Honduras, Guatemala, Nicaragua, Panamá y Colombia– por un valor de cinco millones de dólares. Con esta adquisición, la paraestatal proveerá electricidad a Centroamérica a partir del segundo trimestre del año. La red eléctrica que irá de México a Panamá llevará una fibra óptica como la que tiene el sistema eléctrico mexicano, y servirá para ofrecer servicios de voz y datos en esos países. A febrero de 2009 ya se había avanzado un 40% en la instalación de la red eléctrica de interconexión.
Estamos mal en banda ancha	Los servicios de banda ancha en México tienen tan mala calidad que se sitúan entre los peores del mundo. Según el primer estudio cualitativo de los servicios de Internet, desarrollado por las universidades de Oxford y Oviedo, México se ubica en el lugar 40 de 42 países analizados y el rendimiento de la banda ancha no tiene la capacidad para cumplir con la demanda de las aplicaciones web actuales ni futuras. El primer lugar fue para Japón, que tiene una estrategia de llevar fibra óptica para acceso del hogar.

Estos sólo son algunos aspectos generales que se han llevado a cabo, hay que considerar que México cuenta con diversas organizaciones encargadas del mejoramiento de la seguridad informática, como por ejemplo AMIPCI (Asociación Mexicana de Internet), ALAPSI (Asociación Latinoamericana de Profesionales en Seguridad Informática), DGSCA-UNAM (Dirección General de Servicios de Cómputo Académico), Dirección de Informática IPN, CUDI (Corporación Universitaria para el desarrollo de Internet A.C.), AMITI (Asociación Mexicana de la Industria de Tecnologías de Información), entre otras, pero el objetivo principal de todas estas organizaciones, es desarrollar e investigar nuevas tecnologías, ayudando a mitigar las amenazas a las que se enfrentan todas las organizaciones, ayudándoles a proteger el valor más preciado para éstas, que es la información.

Capítulo 2

Amenazas y vulnerabilidades de la seguridad informática

A finales de la década de los 80's las amenazas y vulnerabilidades a la seguridad informática eran objetos fáciles de identificar ya que las redes eran de uso exclusivo del ejercito militar de los Estados Unidos, pero poco a poco éstas fueron evolucionando hasta convertirse en una herramienta de uso común para las empresas, escuelas y hogares. Cabe destacar que los ataques que se llegaban a efectuar anteriormente eran muy peligrosos, lo que sucede en esta época, es que las nuevas amenazas ahora son más sofisticadas, ya que cuentan con una gran cantidad de variantes, un periodo de vida y distribución más corto, generalmente tienen un mayor alcance y provocan más daño, esto se ha ido dando de forma paralela con el crecimiento de la tecnología porque ahora hay mas personas dedicadas a burlar los sistemas de seguridad de las organizaciones o de cualquier usuario que tenga acceso a una red de computadoras.

Por lo tanto en este capítulo se explican los conceptos de "amenaza" y "vulnerabilidad", se dan a conocer las principales amenazas y vulnerabilidades que se han detectado desde sus inicios hasta el primer semestre del año 2009 así como su evolución y los daños que pueden causar si se llegan a efectuar.

Capítulo 2. Amenazas y vulnerabilidades de la seguridad informática

2.1 Clasificación general de amenazas

En el campo de la seguridad informática se maneja mucho el término de "*amenaza*". El diccionario de la lengua española la define como el *"anuncio de un mal o peligro"*[25].
En términos generales, existen dos tipos de amenazas, las que provienen de sucesos naturales, como por ejemplo; terremotos, incendios forestales, huracanes, inundaciones, sequías, plagas, tsunamis y tornados y las amenazas provocadas por la actividad humana, como las explosiones, los incendios, los derrames de sustancias tóxicas, las guerras, el terrorismo, entre otros.

Dentro de las amenazas provocadas por la actividad humana relacionada con la seguridad informática, se puede decir que, *una amenaza representa la acción que tiende a causar un daño a los dispositivos o sistemas en donde se encuentra almacenada la información, atentando contra su confidencialidad, integridad y disponibilidad.*

Si una amenaza se llega a efectuar, ocurren diversos casos como por ejemplo; interrupción de un servicio o procesamiento de un sistema, modificación o eliminación de la información, daños físicos, robo del equipo y medios de almacenamiento de la información, entre otros. Las amenazas a la seguridad informática se clasifican en humanas, lógicas y físicas.

2.1.1 Humanas

Estos ataques provienen de individuos que de manera intencionada o no, causan enormes pérdidas aprovechando alguna de las vulnerabilidades que los sistemas puedan presentar. A estas personas se les bautizó de la siguiente manera, derivado del perfil que presenta cada individuo y para el presente trabajo únicamente se dan a conocer las más importantes las cuales se describen a continuación:

[25] http://diccionarios.elmundo.es/diccionarios/cgi/lee_diccionario.html?busca=amenaza&diccionario=1

- **Hacker:** Persona que vive para aprender y todo para él es un reto, es curioso y paciente, no se mete en el sistema para borrarlo o para vender lo que consiga, quiere aprender y satisfacer su curiosidad. Crea más no destruye.
- **Cracker:** Es un hacker cuyas intenciones van más allá de la investigación, es una persona que tiene fines maliciosos, demuestran sus habilidades de forma equivocada ó simplemente hacen daño sólo por diversión.
- **Phreakers:** Personas con un amplio conocimiento en telefonía, aprovechan los errores de seguridad de las compañías telefónicas para realizar llamadas gratuitas.

No se necesita ser un hacker para realizar alguna acción maliciosa a los sistemas de información, muchas veces un individuo puede realizar una acción indebida por diversión, por desconocimiento, entre otros. Hay que recordar que el talón de Aquiles de una empresa es su propio personal, es por ello que han surgido nuevos sistemas de ataque, los cuales se describen a continuación:

- **Ingeniería social:** Un atacante utiliza la interacción humana o habilidad social para obtener información comprometedora acerca de una organización, de una persona o de un sistema de cómputo. El atacante hace todo lo posible para hacerse pasar por una persona modesta y respetable, por ejemplo, pretende ser un nuevo empleado, un técnico de reparación, un investigador, etc.
- **Ingeniería social inversa:** El atacante demuestra de alguna manera que es capaz de brindar ayuda a los usuarios y estos lo llaman ante algún imprevisto, aprovechando la oportunidad para pedir la información necesaria y así solucionar el problema tanto del usuario como el propio.
- **Trashing (cartoneo):** Generalmente, un usuario anota su login y pasword en un papelito y luego, cuando lo recuerda, lo arroja a la basura. El trashing puede ser físico (como el que se describió) o lógico, como analizar buffers de impresora y memoria bloques de discos, entre otros.
- **Terroristas:** No se debe de entender a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él.

- **Robo:** La información contenida en los equipos de cómputo puede copiarse fácilmente, al igual que los discos magnéticos y el software.
- **Intrusos remunerados:** Es el grupo de atacantes de un sistema más peligroso aunque es el menos habitual en las redes normales ya que suele afectar más a las grandes empresas u organismos de defensa. Se trata de personas con gran experiencia en problemas de seguridad y con un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos o simplemente dañar la imagen de la entidad afectada.
- **Personal interno:** Son las amenazas al sistema, provenientes del personal del propio sistema informático, rara vez es tomado en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Este tipo de de ataque puede ser causado de manera intencional o sin dolo.
- **Ex–Empleados:** Se trata de personas descontentas con la organización que aprovechan las debilidades de un sistema que conocen perfectamente, para dañarlo como venganza por algún hecho que consideran injusto.
- **Curiosos:** Personas con un alto interés en las nuevas tecnologías, pero no cuentan con la suficiente experiencia para ser considerados como hackers o crackers.
- **Personal interno:** Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta, porque se supone un ámbito de confianza muchas veces inexistente. Estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también son de tipo intencional. Por ejemplo: un electricista puede ser más dañino que el más peligroso de los delincuentes informáticos, ya que un corte de energía puede causar un desastre en los datos del sistema.

2.1.2 Lógicas

En este tipo de amenazas se encuentran una gran variedad de programas que, de una u otra forma, dañan los sistemas creados de manera intencionada (software malicioso conocido como malware) o simplemente por error (bugs o agujeros).

Las amenazas más comunes son:

- **Adware:** Software que durante su funcionamiento despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla.
- **Backdoors:** Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar 'atajos' en los sistemas de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos.
- **Bombas Lógicas:** Son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.
- **Caballos de Troya:** Es aquel programa que se hace pasar por un programa válido cuando en realidad es un programa malicioso. Se llama troyano, caballo de Troya (trojan horse) por la semejanza con el caballo que los griegos utilizaron para disfrazar su identidad y ganar su guerra contra la ciudad de Troya. Así, un usuario podría descargar de un sitio Web de Internet un archivo de música que en realidad es un troyano que instala en su equipo un keylogger o programa que capture todo lo que escriba el usuario desde el teclado y después esta información sea enviada a un atacante remoto.
- **Exploits:** Programa o técnica (del ingles *to exploit*, explotar, aprovechar) que aprovecha una vulnerabilidad. Los exploits dependen de los sistemas operativos y sus configuraciones.
- **Gusanos (Worms):** Programas que se propagan por sí mismos a través de las redes, tomando ventaja de alguna falla o hueco de seguridad en los sistemas operativos o en el software instalado en los equipos de cómputo y que tiene como propósito realizar acciones maliciosas.
- **Malware:** Proviene de la agrupación de las palabras **"Mal**icious Soft**ware".** Este programa o archivo, está diseñado para insertar virus, gusanos, troyanos, spyware o

incluso bots (tipo de troyano que cumple una función específica), intentando conseguir información sobre el usuario o sobre la PC.

- **Pharming:** Consiste en suplantar el Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducir al usuario a una página Web falsa.
- **Phishing:** Es un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador, mejor conocido como *phisher* se hace parar por una persona o empresa de confianza en una aparente comunicación oficial electrónica.
- **Spam:** Mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. La más utilizada entre el público en general es la basada en el correo electrónico. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.
- **Spyware o programas espía:** Se refiere a las aplicaciones que recopilan información sobre una persona u organización, las cuales se instalan y se ejecutan sin el conocimiento del usuario. El objetivo principal del spyware es recolectar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.
- **Virus:** Programas que tienen como objetivo alterar el funcionamiento de la computadora y en ciertos casos alterar la información, se propagan sin el consentimiento y conocimiento del usuario. Algunos de los virus informáticos requieren de la intervención del usuario para comenzar a propagarse, es decir, no se activan por sí mismos, otros no la requieren y se activan solos.

En un principio, los virus se propagaban a través del intercambio de dispositivos de almacenamiento como disquetes y memorias de almacenamiento (USBs). Actualmente un equipo se puede infectar al abrir un archivo adjunto (ya sean documentos, imágenes, juegos, entre otros.) que llegue a través de un correo electrónico.

Los virus se distribuyen a través de mecanismos de intercambio de archivos, es decir, aquellos que se suelen utilizar para distribuir software, música y videos, están diseñados

para afectar a los sistemas operativos. La manera de erradicarlos y de protegerse contra éstos, es a través de un software antivirus, éste vendría siendo de poca ayuda si no se encuentra actualizado.

Dentro de este tipo de ataque (lógico), existen otro tipo de ataques los cuales tienen que ver con los sistemas y se han clasificado de la siguiente manera:

- **Ataques de Autenticación:** Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y Pasword. Algunos de estos ataques son: **Spoofing-Looping** (los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing), **IP Splicing-Hijacking, Spoofing (**Existen los IP Spoofing, DNS spoofing y Web Spoofing), **Net Flooding.**
- **Ataques de Monitorización:** Se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro. Se presentan como: **Shoulder Surfing, Decoy (Señuelos), Scanning (búsqueda), Snooping-Downloading, TCP Connect Scanning, TCP SYN Scanning.**
- **Uso de Diccionarios:** Son archivos con millones de palabras, las cuales pueden ser passwords utilizadas por los usuarios. El programa encargado de probar cada una de las palabras encripta cada una de ellas (mediante el algoritmos utilizado por el sistema atacado) y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema mediante el usuario correspondiente a la clave hallada.
- **Denial of Service (DoS):** Los ataques de denegación de servicio tienen como objetivo saturar los recursos de la víctima, de forma tal que se inhabilitan los servicios brindados por la misma. Ejemplos: **Jamming o Flooding, Syn Flood, Connection Flood, Net Flood, Land Attack, Smurf o Broadcast storm, Supernuke o Winnuke, Teardrop I y II, Newtear-Bonk-Boink, E-mail bombing-Spamming.**

- **Ataques de Modificación-Daño:** Se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Ejemplos de este tipo de Ataques: **Tampering o Data Diddling, Borrado de Huellas. Ataques mediante Java Applets, Ataques Mediante JavaScript y VBScript, Ataques Mediante Active X, Ataques por Vulnerabilidades en los Navegadores.**

2.1.3 Físicos

Este tipo de ataque está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en el cual se encuentran ubicados los centros de cómputo de cada organización o individuo. Las principales amenazas que se prevén en la seguridad física son:

1. **Incendios:** Generalmente son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. El fuego es una de las principales amenazas contra la seguridad porque es considerado como el enemigo número uno de las computadoras debido a que puede destruir fácilmente los archivos de información y programas. Por ello es necesario proteger los equipos de cómputo, instalándolos en áreas que cuenten con los mecanismos de ventilación y detección adecuados contra incendios y que únicamente ingrese el personal autorizado.
2. **Inundaciones:** Se define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.
3. **Terremotos:** Fenómenos sísmicos que pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas.
4. **Señales de Radar:** Las señales muy fuertes de radar infieren en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 volts/Metro o mayor. Ello podría ocurrir sólo si la

antena respectiva fuera visible dese una ventana del centro de procesamiento respectivo y en algún momento estuviera apuntando directamente hacia dicha ventana.

5. **Instalaciones eléctricas:** Trabajar con computadoras implica trabajar con electricidad. En las instalaciones eléctricas se debe considerar los siguientes aspectos: picos y ruidos electromagnéticos, buen cableado, pisos de placas extraíbles, un buen sistema de aire acondicionado, emisiones electromagnéticas.

Esta clasificación, de los principales ataques a la seguridad informática van muy ligadas, son aspectos que no deben pasar desapercibidas en ninguna organización ya que conforman la base para tener una buena estructura de seguridad, si alguna de éstas falla, no se podrá tener la certeza de mantener protegida la información, lo que puede provocar grandes daños tanto económicos.

2.2 Clasificación general de vulnerabilidades

En materia de seguridad informática los puntos débiles de los sistemas son comúnmente aprovechados por personas que buscan la manera de acceder y realizar alguna acción maliciosa para su propio beneficio, desgraciadamente todos los sistemas tecnológicos presentan alguna debilidad, por ejemplo, los sistemas requieren de energía eléctrica, sin ella simplemente no funcionan.

Es por ello que es muy importante conocer esos puntos débiles, una vez identificados, las empresas definen las medidas de seguridad adecuadas con la finalidad de reducir los riesgos a los que pueda estar sometida, evitando que se efectúe una amenaza.

Estos puntos débiles se conocen como *vulnerabilidades*, el diccionario de la real academia de la lengua española define la palabra vulnerable como: *"Que puede ser herido o recibir lesión física o moralmente"*. [26] En materia de seguridad informática las vulnerabilidades

[26] http://diccionarios.elmundo.es/diccionarios/cgi/lee_diccionario.html?busca=vulnerable&diccionario=1

son las debilidades de los activos de las organizaciones, las cuales podrían ser utilizadas por las amenazas para causar daño a los sistemas.

En la figura 2.1 se muestra una clasificación de las principales vulnerabilidades a las que las organizaciones están expuestas:

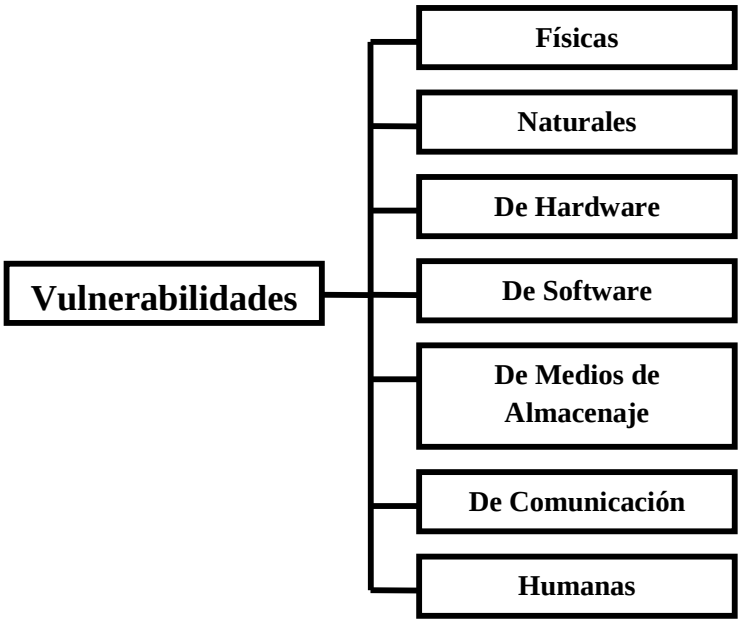


Figura 2.1 Principales Vulnerabilidades

A continuación se describirán de manera general cada uno de los diferentes tipos de vulnerabilidades:

- **Vulnerabilidad física**: Se refiere al lugar en donde se encuentra almacenada la información, cómo los centros de cómputo. Para un atacante le puede resultar más sencillo acceder a la información que se encuentra en los equipos que intentar acceder vía lógica a éstos o también se puede dar el caso de que al acceder a los centros de cómputo el atacante quite el suministro de energía eléctrica, desconecte cables y robe equipos. Si este tipo de vulnerabilidad se llega a efectuar, afecta a uno de los principios básicos de la seguridad informática que es la disponibilidad.
- **Vulnerabilidad natural:** Se refiere a todo lo relacionado con las condiciones de la naturaleza que ponen en riesgo la información. Por ejemplo, incendios, inundaciones, terremotos, huracanes, entre otros. Por ello es conveniente contar con

las medidas adecuadas, como tener respaldos, fuentes de energía alterna y buenos sistemas de ventilación, para garantizar el buen funcionamiento de los equipos.

- **Vulnerabilidad de hardware:** Hacen referencia a los posibles defectos de fábrica o a la mala configuración de los equipos de cómputo de la empresa que puedan permitir un ataque o alteración de éstos. Por ejemplo; la falta de actualización de los equipos que se utilizan o la mala conservación de los equipos son factores de riesgo para las empresas.
- **Vulnerabilidad de software:** Está relacionado con los accesos indebidos a los sistemas informáticos sin el conocimiento del usuario o del administrador de red. Por ejemplo; la mala configuración e instalación de los programas de computadora, pueden llevar a un uso abusivo de los recursos por parte de usuarios mal intencionados. Los sistemas operativos son vulnerables ya que ofrecen una interfaz para su configuración y organización en un ambiente tecnológico y se realizan alteraciones en la estructura de una computadora o de una red.
    - **Vulnerabilidad de medios de almacenaje:** Son los soportes físicos o magnéticos que se utilizan para almacenar la información. Por ejemplo; los disquetes, cd-roms, cintas magnéticas, discos duros, entre otros. Por lo tanto si estos soportes no se utilizan de manera adecuada, el contenido de los mismos podrá ser vulnerable a una serie de factores que afectan la integridad, disponibilidad y confidencialidad de la información.
    - **Vulnerabilidad de comunicación:** Es el trayecto de la información, es decir, donde sea que la información viaje, ya sea vía cable, satélite, fibra óptica u ondas de radio, debe existir seguridad. El éxito en el tránsito de los datos es un aspecto crucial en la implementación de la seguridad de la información por lo tanto se debe evitar:
        - Cualquier falla en la comunicación que provoque que la información no esté disponible para los usuarios, o por el contrario, que esté disponible para quien no tiene autorización.
        - Que la información sea alterada afectando la integridad de ésta.
        - Que la información sea capturada por usuarios no autorizados, afectando su confidencialidad.

- **Vulnerabilidad humana:** Se refiere a los daños que las personas puedan causar a la información y al ambiente tecnológico que la soporta sea de manera intencional o no. Muchas veces los errores y accidentes que amenazan a la seguridad de la información ocurren en ambientes institucionales, la principal vulnerabilidad es la falta de capacitación y la falta de conciencia de seguridad para las actividades de rutina, los errores, omisiones, etc. También existen las vulnerabilidades humanas de origen externo, como son; el vandalismo, estafas, invasiones, etc.

Las vulnerabilidades están ligadas a los hombres, a los equipos y al entorno. Por ejemplo, en cualquier organización de nada serviría tener herramientas de seguridad como (firewall's, IDS, antivirus, entre otros) si los centros de cómputo estuviesen en un lugar inadecuado y accesible a cualquier gente, ya que se está expuesto a que cualquier individuo realice un uso indebido a los equipos provocando grandes daños.

Existen otros tipos de vulnerabilidades que también afectan a las organizaciones a nivel mundial, pero que muy difícilmente se toman en cuenta, estas son:

1. **Vulnerabilidad de tipo Económico:** Se refiere a la escasez y un mal manejo de los recursos destinados a las organizaciones para el mejoramiento de las diversas áreas.
2. **Vulnerabilidad de tipo Socio-Educativa:** Se refiere a las relaciones, comportamientos, métodos y conductas de todas aquellas personas que tienen acceso a una red y lo que deseen de ésta.
3. **Vulnerabilidad de tipo Institucional/Política:** Se refiere a los procesos, organizaciones, burocracia, corrupción y autonomía que tienen todos los países del mundo. Desgraciadamente un atacante puede someter a ciertas personas a revelar información, realizando actos de corrupción.

Por lo anterior mencionado se puede decir que una vulnerabilidad es el paso previo a que se efectúe una amenaza, ésta se encuentra presente en todo momento, pero se reducen los riesgos teniendo en cuenta buenas medidas de seguridad.

Es recomendable que las empresas realicen análisis de riesgos detallado de las vulnerabilidades a las que están expuestos, como las físicas, de software, humanas, entre otros, para evitar en la medida de lo posible ser puntos blancos de ataque.
Es muy importante ser consciente de que por más que las empresas sean las más seguras desde el punto de vista de ataques externos, Hackers, virus, entre otros, la seguridad de la misma sería nula si no se ha previsto como combatir un incendio.
Por ello se hace mucho hincapié sobre la importancia de la seguridad informática, ya que se está invirtiendo para proteger el objeto más valioso de cualquier empresa, que es *la información.*

2.3 Identificación de las principales amenazas y vulnerabilidades a nivel Nacional e Internacional

Conforme ha ido avanzando la tecnología en el mundo de la seguridad informática, las amenazas se han vuelto cada vez más sofisticadas y en ocasiones han sido difíciles de detectar, lo que implica estar al día y tener conocimiento de las nuevas amenazas que van surgiendo, buscando la manera de mantener los sistemas actualizados para evitar que alguna de estas amenazas se lleve a cabo con éxito.

Por este motivo, para el presente trabajo se realizó un análisis basado en estudios e informes presentados por las empresas PandaLabs, PandaSecurity, McAfee, Sophos y la UNAM-CERT, sobre las principales amenazas y vulnerabilidades que se han presentado hasta el año 2009 y algunos comparativos con años anteriores.

En primera instancia es necesario conocer las principales amenazas de mayor peligro que se han efectuado en los últimos 20 años, esta recopilación la realizó la empresa PandaSecurity y se basó en la capacidad de distribución epidémica y daño causado tanto a usuarios domésticos como a las diversas organizaciones. A continuación en la tabla 2.1 se muestran estos acontecimientos.

Tabla 2.1. Las amenazas más peligrosas en los últimos 20 años

Año	Amenaza	Característica
1988	Viernes 13 ó Jerusalén	Creada en Israel y detectada por primera vez en la ciudad de Jerusalén. La creación de esta amenaza estaba relacionada con el aniversario de la fundación del Estado de Israel, aunque coincidió que apareció un viernes 13. Este virus infectaba archivos .COM y .EXE.
1993	Barrotes	Se trata del primer virus en español. El virus se hospedaba en la PC para activarse en enero 5, cuando desplegaría unas barras tipo barrotes en la pantalla.
1997	Cascada o letras cayendo	Creado en Alemania, provocaba que las letras proyectadas en la pantalla cayeran en cascada una vez que la PC fuera infectada.
1998	CIH o Chernobyl	Producido en Taiwán, tan solo le tomó una semana distribuirse para infectar miles y miles de PC's. El virus infecta los archivos ejecutables de 32 bits de Windows 95/98.
1996	Melissa	Detectado en EU. Fue uno de los primeros en utilizar con gran éxito las tácticas de ingeniería social para su distribución masiva, llegaba al buzón de los correos con el texto "Aquí está el documento que me pediste… no se lo muestres a nadie más".
2000	I love you o Love letter	El muy popular virus salió de Filipinas y fue distribuido con el asunto "ILoveYou". Millones de PC's fueron infectadas en todo el mundo en solo unas semanas y su alcance fue tan amplio que golpeó al mismo Pentágono.
2001	Klez	Fue creado en Alemania y solo infectaba computadoras los días 13 de cada mes non. Nimda: Es 'admin' escrito al revés. Su poder consistió en conseguir privilegios de administrador al infectar PC's. Apareció en China.
2003	SQLSlammer Blaster Sobig	-Fue un gran dolor de cabeza para las empresas pues en sólo unos días afecto a más de 500,000 servidores. -Contenía dos mensajes escondidos en su código, uno decía "I just want tos ay love you, San!" y "Billy gates, why do you make this posible? Stop making money and fix your software". -Este virus fue muy famoso y vino acompañado de numerosas variantes, de las cuales la F fue la más dañina, generando millones de copias de sí mismo.
2004	Bagle Netsky	-Este ejemplar y sus variantes rondan e infectan las PC's lo que lo convierte en uno de los virus más prolíficos. -Se cree que este gusano provino de Alemania. Su función era explotar vulnerabilidades de Internet Explorer.
2008	Conficker	Se cree que la finalidad de este gusano que ha infectado decenas de millones de PC's junto con sus variantes, ha sido armar una gran red de computadoras zombie.

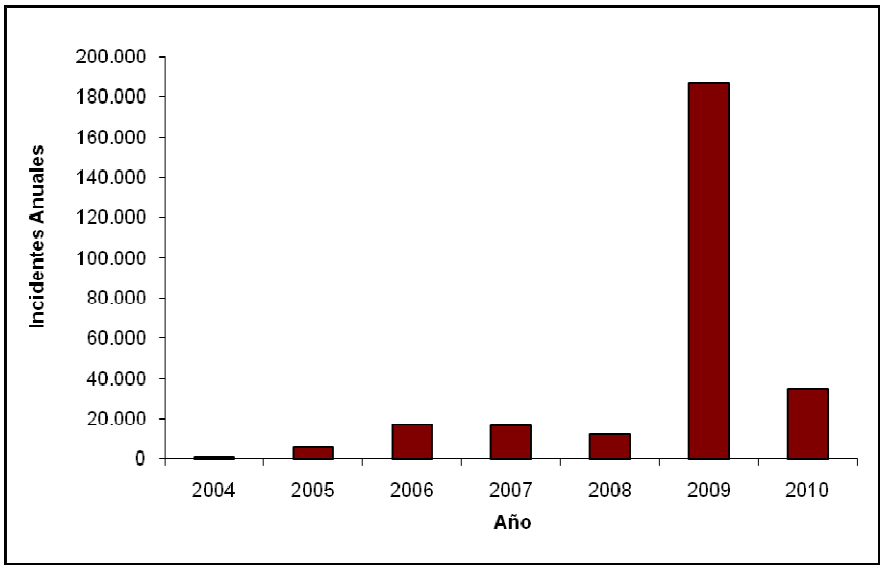
A través de los años, las amenazas a los sistemas de información se han vuelto más sofisticadas llegando a causar un mayor daño a las empresas o a los usuarios comunes, por ello es necesario hacer conciencia sobre la peligrosidad que se puede tener cuando se logre con éxito una amenaza.

En nuestro país la Universidad Nacional Autónoma de México (UNAM) y el Equipo de Respuesta a Incidentes de Seguridad en Cómputo (CERT) el cual, se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún "ataque", así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo ayudando a mejorar la seguridad de los sitios. Dieron a conocer los principales incidentes que se han producido en los últimos años (2004 - 2010).

En la gráfica 2.1 se aprecia que en el año 2004 se reportaron 1,060 incidentes, para el año 2005 y 2006 hubo un incremento de 6,742 y 17,016 incidentes respectivamente, así mismo del 2007 al 2008 disminuyeron de 16,778 a 12,595 incidentes. Se puede observar que para el año 2009 se incrementaron drásticamente el número de incidentes hasta llegar a los 187,393 y finalmente se logró disminuirlos en el año 2010 a 34,908.

Incidentes Anuales

Año	Incidentes
2004	1,060
2005	6,472
2006	17,016
2007	16,778
2008	12,595
2009	187,393
2010	34,908

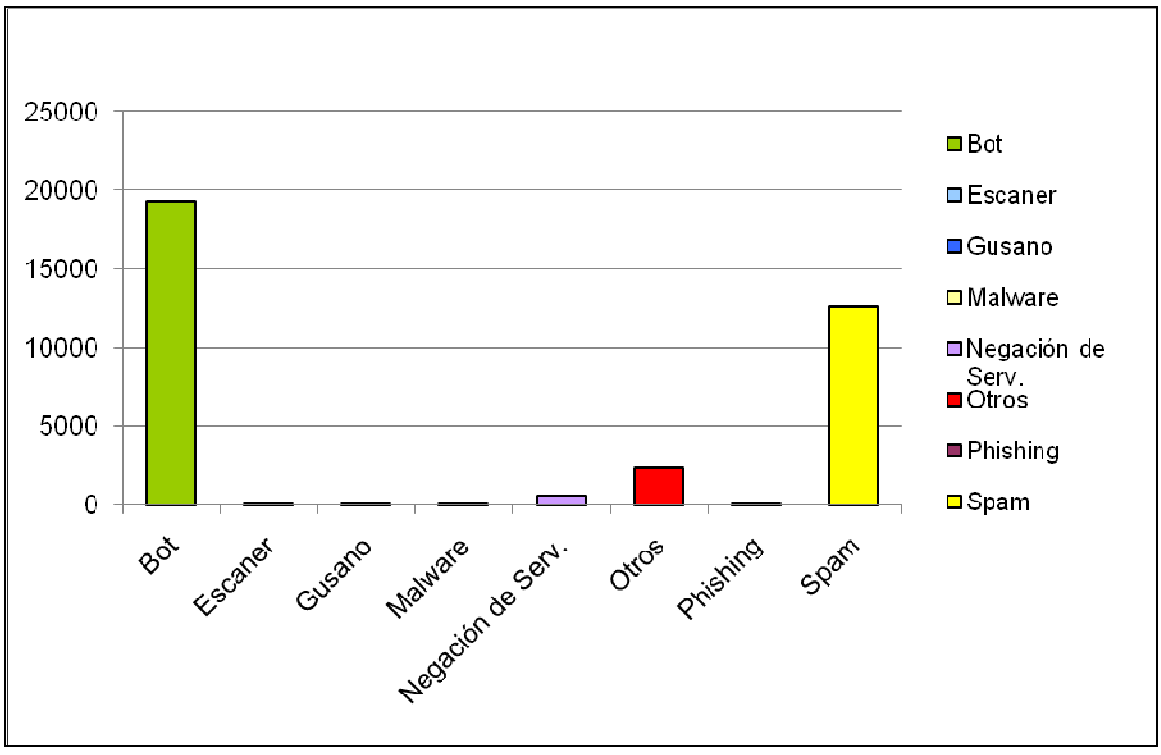


Gráfica 2.1 Incidentes Anuales

Los principales incidentes que se reportaron en el año 2010 fueron los bots y el spam. En la gráfica 2.2 se observa que los bots alcanzaron un total de 19,318 incidentes durante el 2010, así mismo el spam obtuvo 12,626 incidentes y en último lugar lo ocupan los gusanos con tan sólo un incidente anual.

Incidentes Anuales

Reporte	Incidente	%
Bot	19,318	35.5
Escaner	24	.04
Gusano	1	.001
Malware	2	.003
Negación de Servicio	572	1.05
Otros	2,357	4.34
Phishing	8	0.014
Spam	12,626	23.26

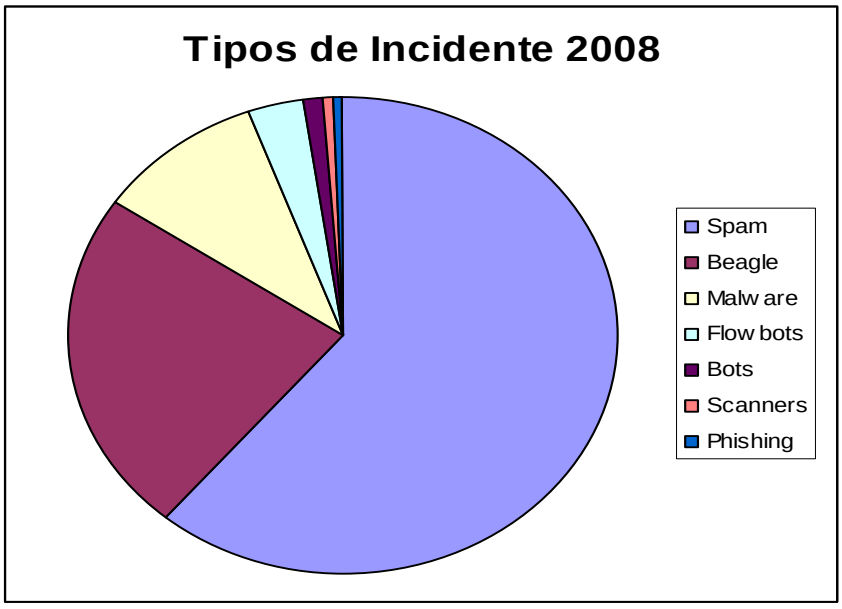


Gráfica 2.2 Tipos de incidentes en el 2010

Los principales incidentes que se reportaron en el año 2008 fueron el spam, beagle (gusano), malware, flowbots (virus), bots (virus), scanners y phishing. En la gráfica 2.3 se observa que el Spam ocupa el 60.56% de todos los incidentes generados en ese año, después le sigue el Beagle con un 23% y en último lugar se encuentra el phishing ocupando el 0.5%.

Principales Problemas

Reporte	%
Spam	60.56
Beagle	23.28
Malware	9.75
Flowbots	3.23
Bots	1.19
Scanners	0.63
Phishing	0.5

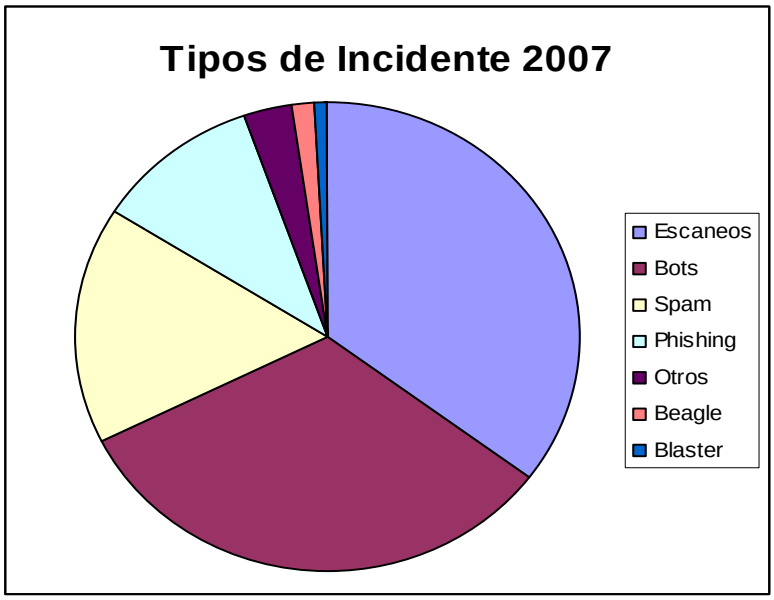


Gráfica 2.3 Tipos de Incidente en el 2008

Para el año 2007 se puede observar en la gráfica 2.4 que el principal incidente fueron los escaneos, ocupando el 35.4% muy a la par de los bots con el 32.16%, el spam se encontraba en tercer lugar con el 16.28% y en último lugar se encontró el blaster (virus) representando el 0.85%

Principales problemas

Reporte	%
Escaneos	35.40
Bots	32.16
Spam	16.28
Phishing	10.91
Otros	3.01
Beagle	1.39
Blaster	0.85

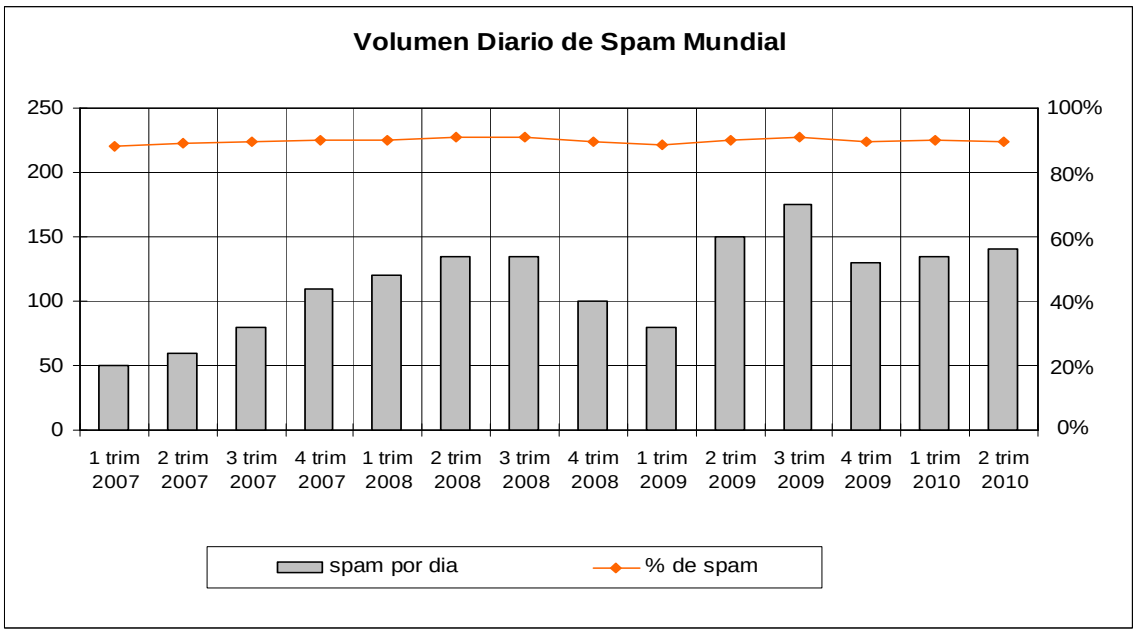


Gráfica 2.4 Tipos de incidente en el 2007

Analizando ambas gráficas se puede observar que, los principales problemas que se presentaron en el año 2007 y 2008 fueron el spam, el beagle, el malware, los flowbots, los bots, scanners, el phishing entre otros. Por otra parte en el año 2007 fueron los escaneos con un 37% pero para el año 2008 disminuyó al 0.63%, en ese mismo año el spam representaba el 16.28% pero en el 2008 éste se incrementó, representando el 60.56%, ocupando el primer lugar en incidentes detectados. En estos años hubo una notable diferencia con respecto a los tipos de ataques que se detectaron, algunos de éstos se incrementaron de manera considerable y otros disminuyeron drásticamente.

Análisis del informe trimestral comprendido del periodo (Abril - Junio) del 2009 realizado por la empresa McAfee sobre amenazas de seguridad informática

En este informe se presentan las últimas estadísticas y análisis acerca de las amenazas que llegan a través del correo electrónico y la web. En la gráfica 2.5 se muestra el porcentaje de spam desde el último trimestre del 2007 al segundo trimestre del 2010.



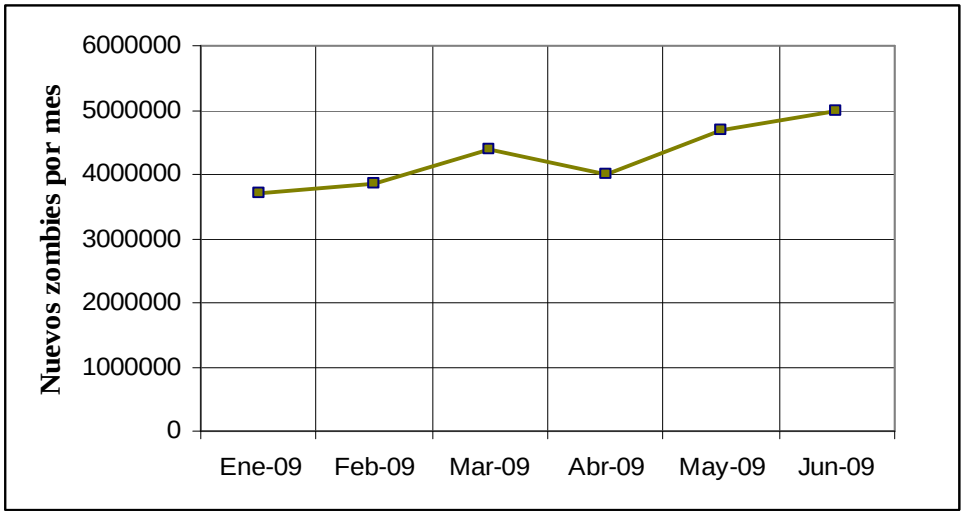
Gráfica 2.5 Volúmenes de spam mundiales y el spam como un porcentaje de todo el correo

Durante el 2do trimestre del año 2010 el tráfico de spam representó el 88% de todo el tráfico de correo electrónico en Internet, un porcentaje ligeramente inferior que en el trimestre anterior.

En general, el spam parece que recupera la tendencia ascendente, aunque de forma lenta, tras la caída del 20% sufrida entre el tercer y cuarto trimestre del año 2009, precisamente en ese trimestre se registró el mayor volumen de spam con casi 175,000 millones de mensajes diarios.

Zombies

En este informe se analizaron lo que hoy en día se conocen como "zombis". Un **zombie** es la denominación que se asigna a computadoras tras haber sido infectadas por algún tipo de malware (el nombre procede de los zombis o muertos vivientes esclavizados). Existen grupos organizados que llegan a controlar decenas de miles de computadoras infectadas (zombis), que usan para generar grandes cantidades de tráfico proveniente de una multitud de diversas fuentes en Internet, dirigido a una sola red o servidor. Otro uso frecuente de los zombis es el envío de spam. En la gráfica 2.6 se muestra el incremento de zombis durante el año 2009, llegando a producir aproximadamente 5 millones de éstos.



Gráfica 2.6 Nuevos zombis que envían spam, por mes

Este problema va acompañado del envío de spam, por lo tanto, el spam sigue representando la principal preocupación que tienen las organizaciones en el mundo.

Nuevos zombies

En la tabla 2.2 se muestra una lista de los 10 principales países que producen nuevos zombis comprendido en el periodo de abril a junio del año 2009. Se aprecia que Estados Unidos ocupa el primer lugar con el 15.7%, seguido de China (9.3%) y en último lugar se encuentra España con el 2.6%. Estos países representan el 60.7% de producción de zombies a nivel mundial, lo que significa que el problema depende en gran medida de estos lugares, por lo tanto deben de prestar mas atención para ayudar a mitigar el problema al que están siendo víctimas.

Tabla 2.2 Países productores de nuevos zombis por trimestre

País	%	País	%
Estados Unidos	15.7	Italia	4
China	9.3	República de Corea	3.8
Brasil	8.2	India	3.2
Rusia	5.6	Reino Unido	3
Alemania	5.3	España	2.6

Spam por país

En la tabla 2.3 se muestra una relación de los países que producen mayor porcentaje de spam a nivel mundial. Estos datos se obtuvieron del periodo comprendido entre el primer semestre del año 2009 y cuarto trimestre del 2008.

Tabla 2.3 Países con mayor producción de spam

País	2º trim. 2009 % total	País	1er trim 2009 % total	País	4 º trim 2008 % total
Estados Unidos	25.5	Estados Unidos	35	Estados Unidos	34.3
Brasil	9.8	Brasil	7.3	Brasil	6.5
Turquía	5.8	India	6.9	China	4.8
India	5.6	Rep. de Corea	4.7	India	4.2
Polonia	4.9	China	3.6	Rusia	4.2
Rep. de Corea	4.6	Rusia	3.5	Turquía	3.8
Rusia	2.4	Turquía	3.2	Rep. de Corea	3.7
Rumania	2.3	Tailandia	2.1	España	2.4
España	2.1	Rumania	2	Reino Unido	2.3
Rep. Checa	1.9	Polonia	1.8	Colombia	2
% total del spam mundial	64.9		70		68.3

Del porcentaje total de estos países se puede notar que hubo un descenso del 5% en el segundo trimestre del año 2009 con respecto al primer trimestre de ese mismo año, lo que indica que la disminución de spam aún es lento, falta mucho por hacer, los países tienen que trabajar en ello para evitar seguir siendo puntos blancos de ataque. Sin embargo, el 65% de la producción de spam sigue procediendo de estas diez naciones.

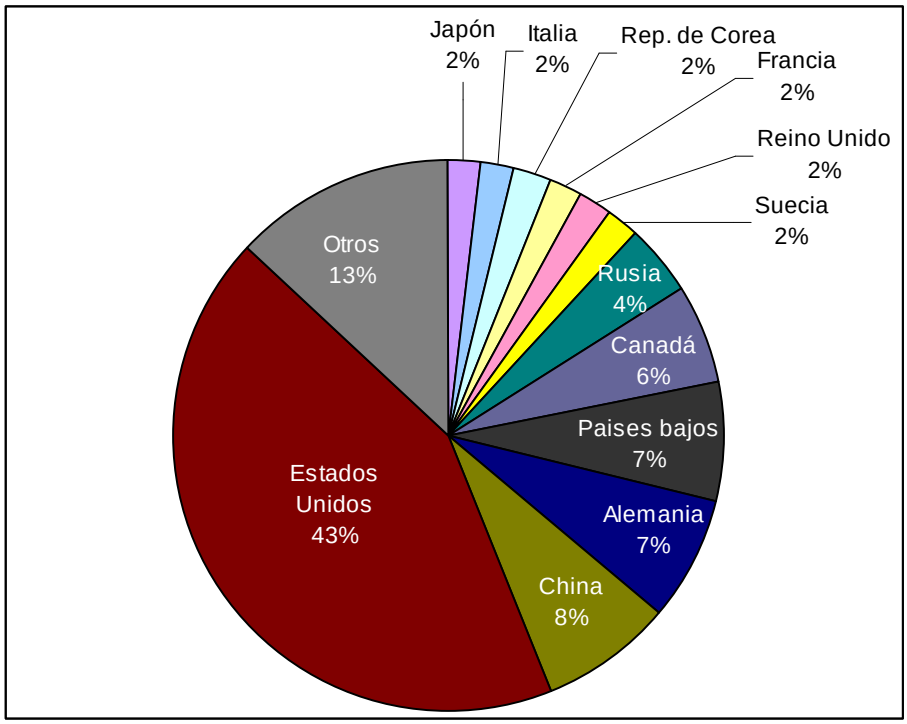
En el último trimestre del 2008 Estados Unidos tenía el 34.3% de spam y para el segundo trimestre del 2009 ocupa el 25.5%, lo que significa que disminuyó aproximadamente un 10% en este periodo. Con lo que respecta a Brasil, sigue manteniendo el segundo lugar con el 9.8% (2trim2009), Turquía se encuentra en el tercer lugar con el 5.8% (2trim2009), a inicios de año estaba en el séptimo lugar, lo que indica que se incrementó el spam en ese país.

Resulta interesante cómo estos países van cambiando su posición en periodos de tiempo muy cortos, se puede decir que, día a día se está en constante lucha contra los ciberdelincuentes, esperando a que estos índices disminuyan considerablemente sin afectar a las organizaciones.

Phishing

Otro problema común en la mayoría de los países es la distribución de sitios web de Phishing, en este caso Estados Unidos abarca el 43%, significa que, ocupa casi el 50% con respecto a los países del mundo, esta cifra es alarmante, puesto que como se ha visto, el mayor problema radica en este país que es una de las principales potencias, por lo tanto, es vulnerable a cualquier tipo de ataque.

En la gráfica 2.7 se observan los países con menor porcentaje de phishing son Japón, Italia, República de Corea, Francia, Reino Unido y Suecia con el 2% respectivamente.

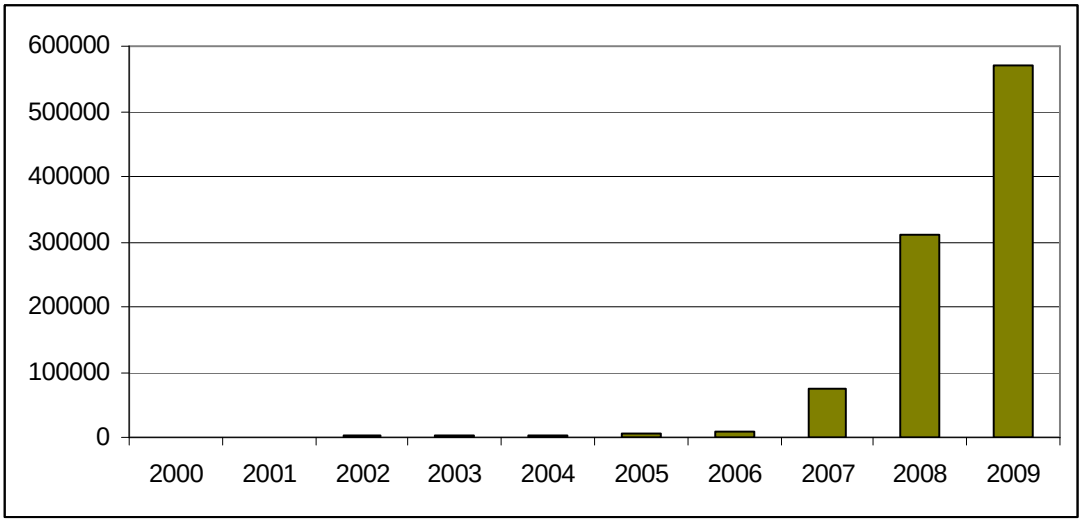


Gráfica 2.7 Distribución de los sitios Web de Phishing

Malware

McAfee señala que el malware y la ciber-delincuencia existen desde los inicios de la informática e Internet. Los virus atacaban el sector de arranque, eran parasitarios y se distribuían principalmente a través de discos flexibles. Aparece el spam y su objetivo era el mismo que tienen hoy día: vender algo. Cuando se produjo la aparición del uso de Internet, el malware y la ciber-delincuencia, evolucionaron para adaptarse a los cambios en el comportamiento de los usuarios. En la actualidad, la vida de muchas personas está completamente ligada al uso de las computadoras, ya sea para pagar facturas online, utilizar blogs o comunicarse con otros en Facebook y Twitter, la realidad es que ahora las personas y sus identidades son digitales. Los creadores de malware y los ciber-delincuentes conocen bien esta dinámica y no se quedan atrás ante esta.

Los troyanos, ladrones de contraseñas, crecen rápidamente y siguen siendo una de las herramientas favoritas de los ciber-delincuentes. Las herramientas para crear estos troyanos están disponibles de forma generalizada en Internet y hay muchos sitios dedicados a venderlas como un servicio, su función es bien sencilla: robar contraseñas, el secreto de su éxito radica en la complejidad del propio troyano. En la gráfica 2.8 se muestra el crecimiento del malware de robo de contraseñas en el periodo comprendido del año 2000-2009.



Gráfica 2.8 Crecimiento del Malware de robo de contraseñas

Claramente se observa que este incremento se disparó a partir del año 2008 registrando más de 300,000 robos de contraseñas y para el 2009 casi se llegaba a cubrir los 600,000 robos de contraseñas en todo el mundo.

En la mayoría de los casos, los troyanos ladrones de contraseñas infectan a usuarios que abren un adjunto de correo electrónico que descarga malware de un sitio Web malicioso, una vez que se encuentran instalados, los troyanos recopilan nombres de usuarios y contraseñas de una gran variedad de programas, como Internet Explorer, sesiones FTP y muchos juegos online.

Los datos de identidades recogidos, se envían a un servidor controlado por los ciber-delincuentes, que los venden a un comprador utilizando distintos medios, como por ejemplo, sitios de subastas o ventas masivas.

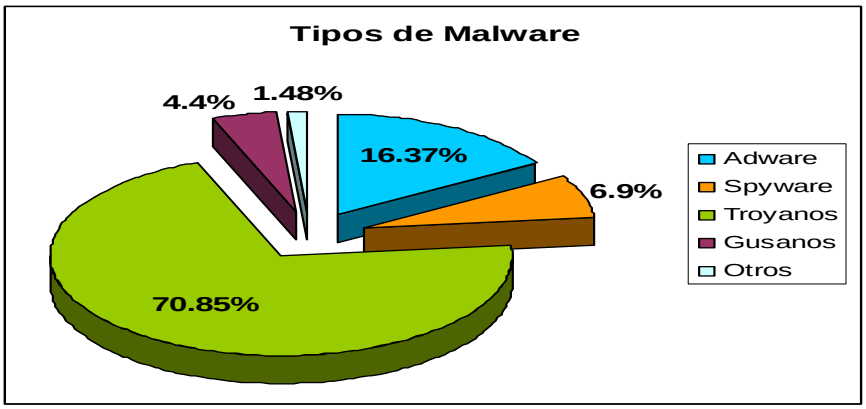
McAfee AvertLabs ha observado que estos programas maliciosos son cada vez más complejos, son más sigilosos que nunca y con frecuencia disponen de mecanismos de autoprotección para garantizar su supervivencia en una PC infectada. Asimismo, cada vez son de índole más general. Antes, los troyanos se creaban específicamente para atacar a una institución concreta. Sin embargo, últimamente han estado recopilando cada vez más datos de una mayor variedad de objetivos, maximizando así su eficacia.

Análisis del informe trimestral comprendido del periodo (Abril – Junio) del 2009 realizado por la empresa PandaLabs.

En este informe se dan a conocer las principales amenazas que afectan a los sistemas de comunicación, así como los principales países que sufren algún tipo de Malware.

Distribución de las nuevas amenazas detectadas

En la gráfica 2.9 se muestran los diferentes tipos de malware detectados durante este periodo. Según los datos presentados por PandaLabs se puede observar que en la categoría de malware predominan los troyanos ocupando el 70.85% seguido del Adware con el 16.37% mientras que los gusanos únicamente ocupan el 4.40%.

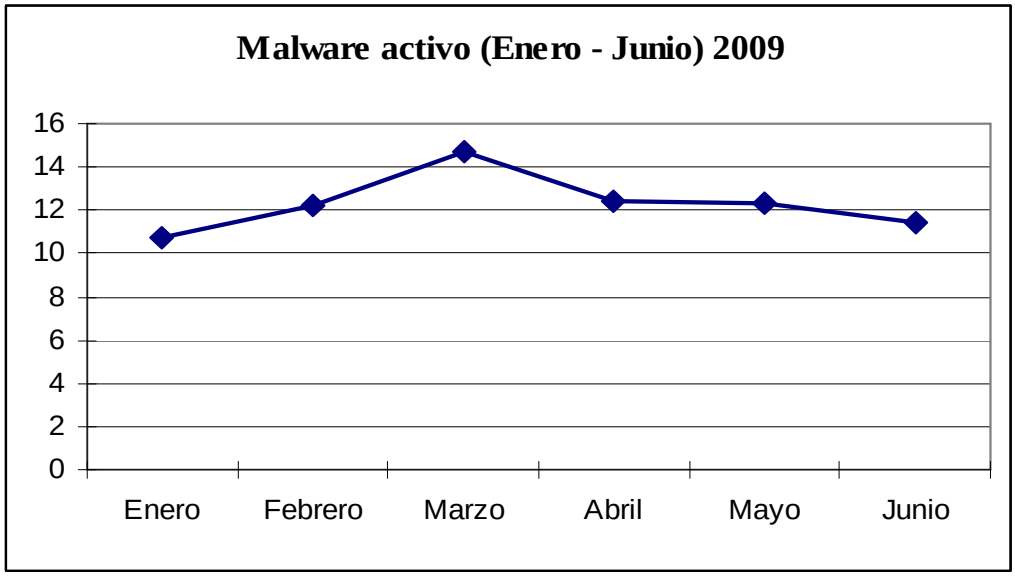


Gráfica 2.9 Tipos de Malware

Malware Activo

PandaLabs define al Malware en dos posibles estados que es el latente y el activo. El malware latente es aquel que está alojado en una máquina pero sin realizar ninguna acción, es decir, está a la espera de ser ejecutado directamente por el usuario o bien de forma remota por el cieberdelincuente, una vez que es ejecutado comienza a realizar las acciones dañinas para las que está programado, por lo tanto, el estado de este malware cambia y pasaría de estar latente a activo.

En la gráfica 2.10 se puede observar la evolución de malware activo durante el primer semestre del 2009. Estos datos se obtuvieron gracias a la herramienta ActiveScan 2.0 proporcionada de manera gratuita a cualquier usuario que ingresaban a la página web de pandalabs: (www.pandasecurity.com/infected_or_not/). De esta manera se comprueba si los equipos están infectados. Los resultados que se recopilaron fueron los siguientes:

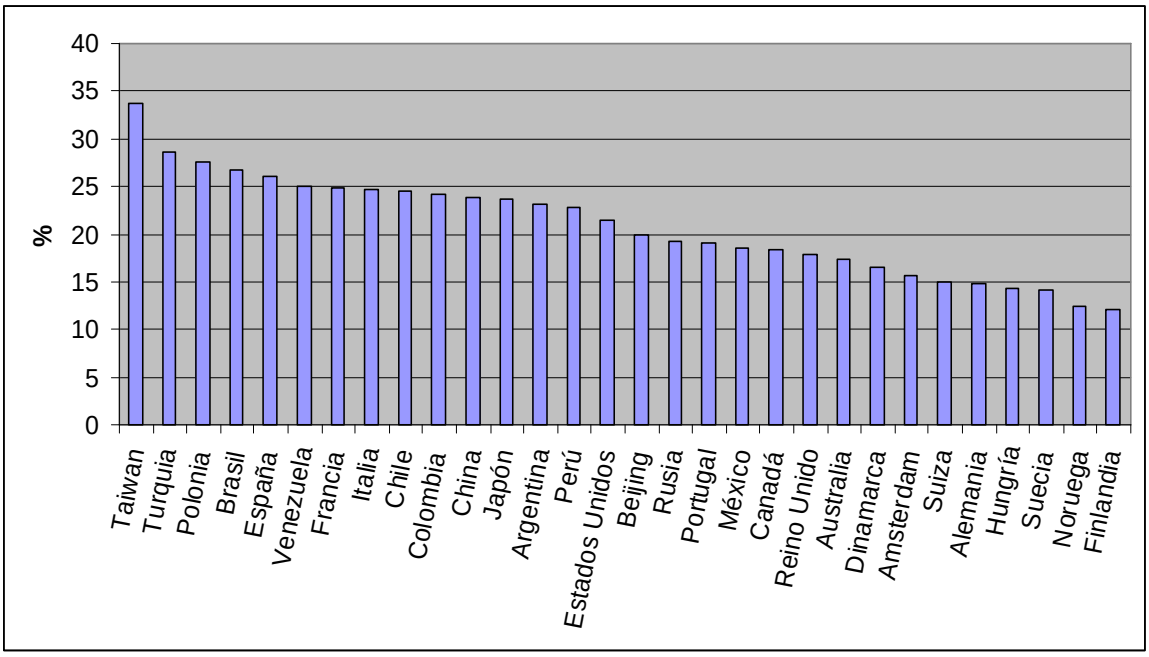


Gráfica 2.10 Evolución de malware activo durante el primer semestre del 2009

Enero mostró un comienzo bajo con el 10.78% de PC's Infectados. Los siguientes dos meses fueron en aumento llegando al 14.68% en marzo, a partir de ahí empezó a disminuir paulatinamente hasta el mes de junio con un 11.39%.

Aunque aún se considera un porcentaje relativamente bajo, es muy importante mantener el control del Malware, de tal manera que se evite en la medida de lo posible que se éste se incremente y para ello se tienen que proporcionar tanto las herramientas adecuadas para solucionar este tipo de amenaza, así como, crear buenos hábitos en los usuarios quienes son los más vulnerables a padecer algún tipo de malware.

En la siguiente gráfica 2.11 se muestra la evolución de máquinas infectadas por país registradas en el primer semestre del año 2009.



Gráfica 2.11 Países con mayor porcentaje de malware (Enero – Junio 2009)

Se puede observar que Taiwan es el país con mayor índice de malware activo, con el 33.63%, por debajo del 30% se encuentra Turquía (28.6%) y Polonia (27.54%). México se encuentra por debajo del 20% seguido de Canadá y del Reino Unido. Los países nórdicos como Suecia (14.2%), Noruega (12.48%) y Finlandia (12.17%) se encuentran con el menor número de PC's infectados de malware activo durante este periodo.

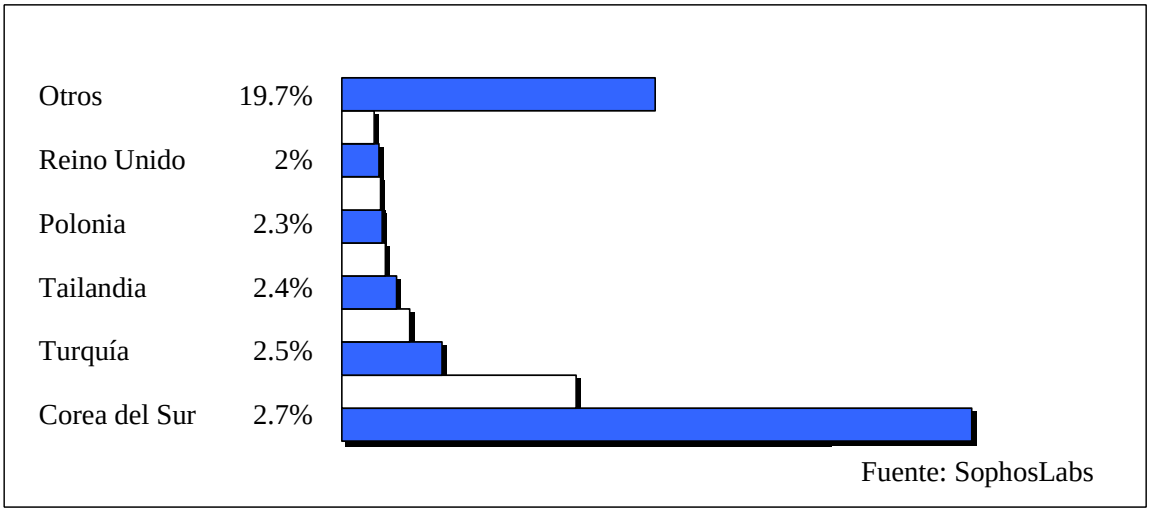
PandaLabs enfatiza que el malware activo a través de los troyanos es el mayor problema que se ha detectado a nivel mundial. México se encuentra en el lugar 19 de 30 países que se

consideraron con el mayor índice de computadoras infectadas, lo que significa que se deben de incrementar las medidas de seguridad para mitigar estos ataques e ir reduciendo este índice, para ello se deben de considerar algunos aspectos como la inversión en materia de seguridad informática y hacer conciencia sobre la situación que se vive a nivel nacional e internacional ya que siempre se está expuesto a sufrir cualquier tipo de incidente.

Análisis realizado por la empresa Sophos durante el primer semestre del 2009

El análisis presentado por la empresa Sophos da a conocer los principales países con mayor cantidad de malware en las páginas web, así como la reproducción de spam por país y por continente.

En la gráfica 2.12 se muestran los países que contienen malware en las páginas web, se observa que Estados Unidos encabeza la lista representado el 39.6%, seguido de China con el 14.7% y en último lugar se encuentra el Reino Unido con el 2%. El resto de los países del mundo representa el 19.7%.

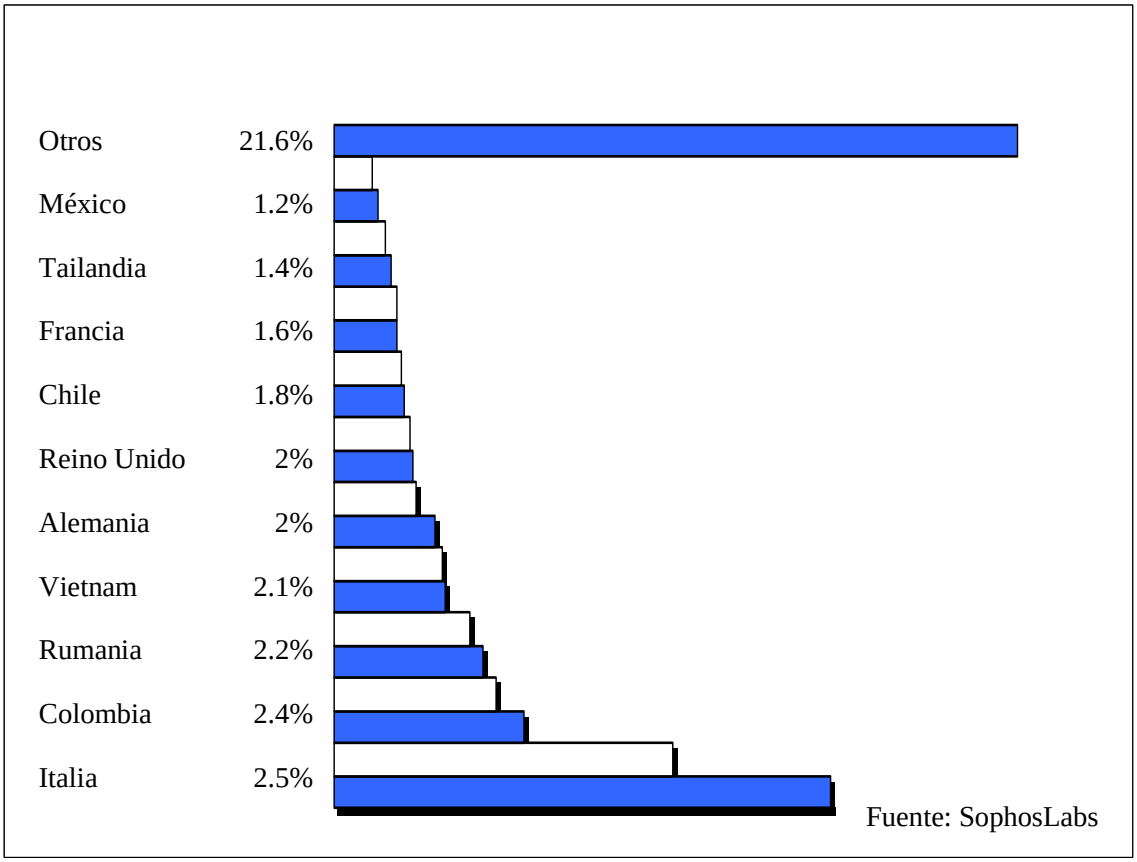


Gráfica 2.12 Países con mayor porcentaje de malware en la web

Prácticamente más de la tercera parte de malware que existe en el mundo, lo padece Estados Unidos, por lo que es necesario prestar mayor atención, incrementar el nivel de seguridad y estar alertas para evitar ser víctimas de cualquier tipo de amenaza.

Reproducción de spam por país

En la gráfica 2.13 se observan los principales países productores de spam, esta lista está conformada por 20 países los cuales representan el 78.4% del total de spam a nivel mundial, el resto representa el 21.6%.

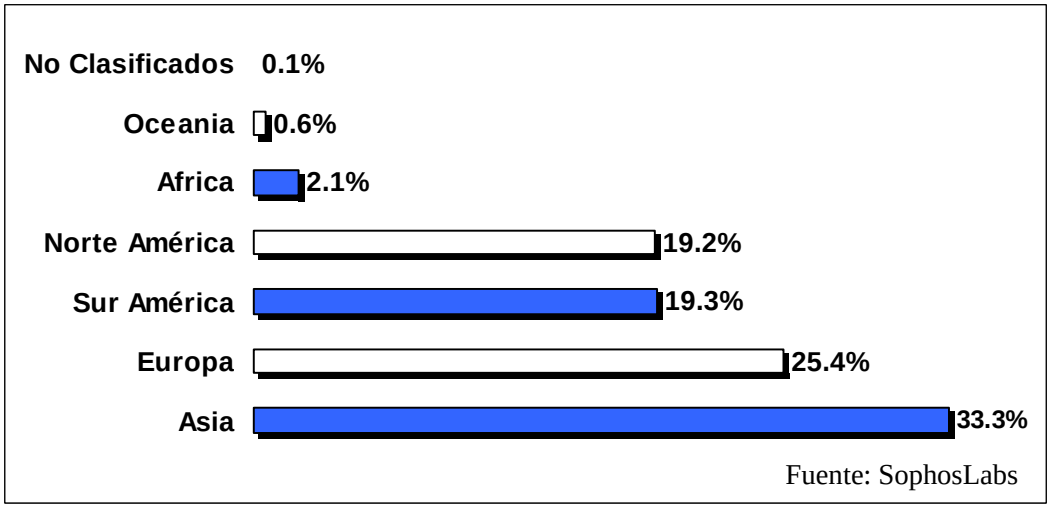


Gráfica 2.13 Reproducción de Spam por país

ShophosLabs señala que Estados Unidos aumentó la cantidad total de spam representando el 15.7% en comparación con el 14.9% en el mismo período del año 2008. Rusia ha caído de su postura anterior en segundo lugar en la tabla (7.5%) hasta el 3.5%. México únicamente representa el 1.2% de spam con respecto a los países en el mundo, por lo tanto se tiene que seguir trabajando para evitar en la medida de lo posible incrementar la reproducción de spam.

Spam por continente

En la gráfica 2.14 se aprecia la cantidad de spam generada por continente en el periodo comprendido de Enero a Junio del año 2009, se puede observar que Asia abarca el 33.3% del total a nivel mundial seguido de Europa. El continente Americano abarca el 19.3% en la parte sur y en la zona norte el 19.2%. Oceanía es el continente que representa tan solo el 0.6% de spam a nivel mundial. Todo se centra en los países desarrollados, derivado del avance de la tecnología.



Gráfica 2.14 Spam por continente

En este informe también se tomaron en cuenta las principales amenazas de seguridad informática que han estado presentes en la primera mitad del 2009, las cuales son:

- **Redes sociales:** Debido al auge que están teniendo estas redes, también se han manifestado sus debilidades, como la falta de privacidad que puede haber si no se configuran adecuadamente, programas maliciosos orientados a estas redes o, como sucede en muchas empresas, pérdida de tiempo por parte de los usuarios y fugas de información.
- **Fuga de información:** Generalmente producida por no tener la información importante cifrada.

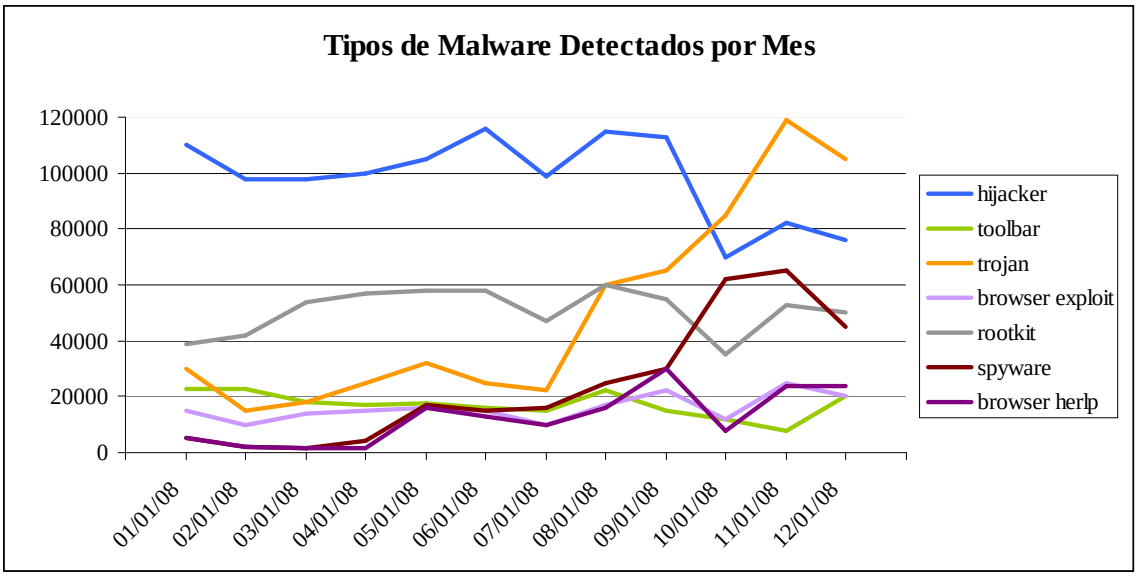
- **Amenazas Web:** Fallos en los navegadores o alguno de sus componentes, enlaces a páginas maliciosas o páginas legítimas que han sido modificadas sin el conocimiento de su creador, son las principales formas de infección.
- **Amenazas de Correo Electrónico:** Los usuarios son vulnerables a quedarse infectados al recibir correos electrónicos que contienen un adjunto malicioso como en correos con enlaces a páginas Web maliciosas.
- **Spam:** Sigue siendo una de las principales molestias a nivel de seguridad informática.
- **Malware:** Este semestre han predominado los falsos antivirus y la infección del gusano Conficker.
- **Apple MACs:** Aunque en menor cantidad que para otras plataformas, este semestre han surgido varios programas maliciosos para MAC.
- **Teléfonos móviles y dispositivos Wi-Fi:** Todas las aplicaciones son susceptibles de ser vulnerables y últimamente se han detectado algunas vulnerabilidades en terminales de gran aceptación entre los usuarios y las empresas como BlackBerry e iPhone.
- **Cibercrimen y delitos informáticos:** Aumenta el ciber-espionaje a la par de que en muchos gobiernos empiezan a arrestar a ciberdelincuentes. Como dato positivo cabe destacar que muchos gobiernos se empiezan a preocupar seriamente por la seguridad informática para prevenir y evitar ciber ataques.

Análisis del informe sobre seguridad informática realizado por la empresa CISCO en el año 2008

En este informe se señalan las principales **vulnerabilidades** que tienen los equipos de comunicación, por ello, los ciber-delincuentes se aprovechan de estas debilidades para instalar malware en los dispositivos y así obtener el control de las computadoras y las redes.

En la gráfica 2.15 se muestra el uso del malware, como troyanos, objetos de ayuda del navegador y software espía. Estos datos reflejan una tendencia muy peligrosa en la

recopilación de datos de malware, así como cada vez más sofisticado el ataque de ingeniería social.



Gráfica 2.15 Tipos de Malware detectados por mes

CISCO presentó de manera general las principales **amenazas** producidas en el primer semestre del año 2009 las cuales se describen a continuación:

- **Botnets:** Estas redes de computadoras sirven como un medio para lanzar un ataque. Los propietarios de los botnets están alquilando estas redes a otros criminales, ofreciendo eficaces y sólidos recursos para suministrar spam y malware.
- **Spam:** El spam sigue siendo un vehículo principal a la hora de expandir gusanos y malware, así como de saturar el tráfico de Internet. Cada día se envían 180,000 millones de mensajes de spam, lo que representa un promedio del 90% de todo el tráfico de correo electrónico del mundo.
- **Gusanos:** El aumento de las redes sociales ha facilitado el lanzamiento de gusanos. La gente que entra en estas comunidades de Internet son más propensos a hacer clic en vínculos y descargar contenido que creen que han enviado personas que conocen y en quienes confían.
- **Indexación de spam:** Muchos tipos de empresas utilizan la optimización de motores de búsqueda para aparecer en listas destacadas en búsquedas realizadas en

Google y otros sitios. La táctica, que implica empaquetar un sitio Web con palabras clave o términos de búsqueda relevantes, se utiliza cada vez más entre los ciber-delincuentes que tratan de disfrazar el malware como software legal, puesto que los usuarios tienden a confiar y no sospechan de las clasificaciones en los principales motores de búsqueda por lo que fácilmente podrían descargar uno de los paquetes de software básicos creyendo que es legal.

- **Fraudes de mensajes de texto:** Desde principios del año 2009 han aparecido al menos, dos o tres campañas semanales, cuyo objetivo son los dispositivos móviles de mano. Cisco describe el creciente mercado de los dispositivos móviles como una *"nueva frontera de fraude irresistible para los criminales"*.
- Con casi 4, 100,000 millones de abonados a teléfonos móviles en todo el mundo, un delincuente podría lanzar una red extraordinariamente amplia y obtener un suculento beneficio, incluso si el ataque se produjera sólo sobre una pequeña parte de los usuarios.
- **Insiders:** La recesión global ha provocado que muchos individuos pierdan su trabajo, como resultado de ello ahora las amenazas provienen de personas que tienen acceso a información confidencial (conocidos como *insiders*), por lo tanto son ya una preocupación para las organizaciones. Estas personas que cometen fraude no sólo podrían ser empleados actuales o ex-empleados, sino contratistas o terceras partes.

Estos análisis ayudan a conocer la problemática que se vive a nivel mundial, en la tabla 2.4 se muestra un resumen sobre los análisis realizados por las diversas organizaciones, y se observa que las principales amenazas a las que se enfrentan los países en el mundo son los escaneos, spam, malware, phishing y bots, lo que ha ocasionado grandes problemas a las empresas e incluso en menor grado a usuarios domésticos derivado del desconocimiento sobre la importancia de mantener protegida la información que manejan.

Tabla 2.4 Resumen de los informes analizados por las diferentes empresas

Año	Organización	País	Tipo de Amenaza	%
2007	UNAM-CERT	México	Escaneos	35.40
			Bot	32.16
2008	UNAM-CERT	México	Spam	60.56
			Beagle	23.28
	Cisco	Todos	Spam	90
2009	McAfee	Todos	Spam	88
		Estados Unidos	Phishing	43
			Spam	25.5
			Zombis	15.7
		Todos	Malware	60
		Brasil	Spam	9.8
		China	Phishing	8
	PandaLabs	Taiwán	Malware	34
		México	Malware	18
	Sophos	Estados Unidos	Malware	39.6
			Spam	25.7
		Brasil	Spam	10.7
		China	Malware	14.7
			Spam	6
2010	UNAM-CERT	México	Bot	35.5
			Spam	23.26

Los resultados presentados por las diversas empresas en materia de seguridad informática colocan a Estados Unidos en el primer lugar con los mayores índices registrados de spam, malware, y phishing principalmente; le siguen Brasil, China, Taiwán, entre otros y en último lugar se encuentran los países con los menores registros de estas amenazas, entre los que se encuentran Rumanía, República Checa, Francia, Italia, México, y Tailandia.

Por lo tanto, para el caso particular de México, los registros presentados indican que está por debajo de los principales países. Esto se debe a muchos factores, como por ejemplo; el tipo de economía, la tecnología que se emplea, el nivel de conocimiento que existe en los usuarios, la educación, entre otros.

Conforme México crece en tecnología, será más vulnerable a sufrir ataques de cualquier índole provenientes de cualquier parte del mundo. Por ese motivo surgió la necesidad de contar con instituciones en materia de seguridad informática las cuales se encargan de mantenerse al día sobre las nuevas amenazas, encontrando soluciones para mitigarlas y así ofrecer un buen sistema de seguridad enfocado a las necesidades de cada empresa o usuario.

Es importante que las empresas inviertan en nuevas metodologías de seguridad para combatir la problemática que se vive en el mundo ya que nadie está exento de sufrir algún ataque y padecer daños que en la mayoría de los casos resultan ser muy costosos.

Por ello, se hace hincapié en que las organizaciones realicen periódicamente un análisis de riesgos para determinar las posibles amenazas y vulnerabilidades a las que se enfrentan, realizando planes de contingencia en los diversos sistemas de seguridad con los que cuenta cada organización. Una vez conocidos los problemas a los que se enfrentan las empresas en el mundo, es recomendable hacer conciencia y proporcionar una adecuada solución a éstos.
Desafortunadamente como se ha mencionado a lo largo de este capítulo, las amenazas y vulnerabilidades van siendo más sofisticadas y difíciles de detectar, se puede decir que existe ahora una guerra cibernética entre aquellos individuos que buscan la manera de llevar a cabo con éxito un ataque de cualquier índole, contra los que se protegen de éstos.

Capítulo 3

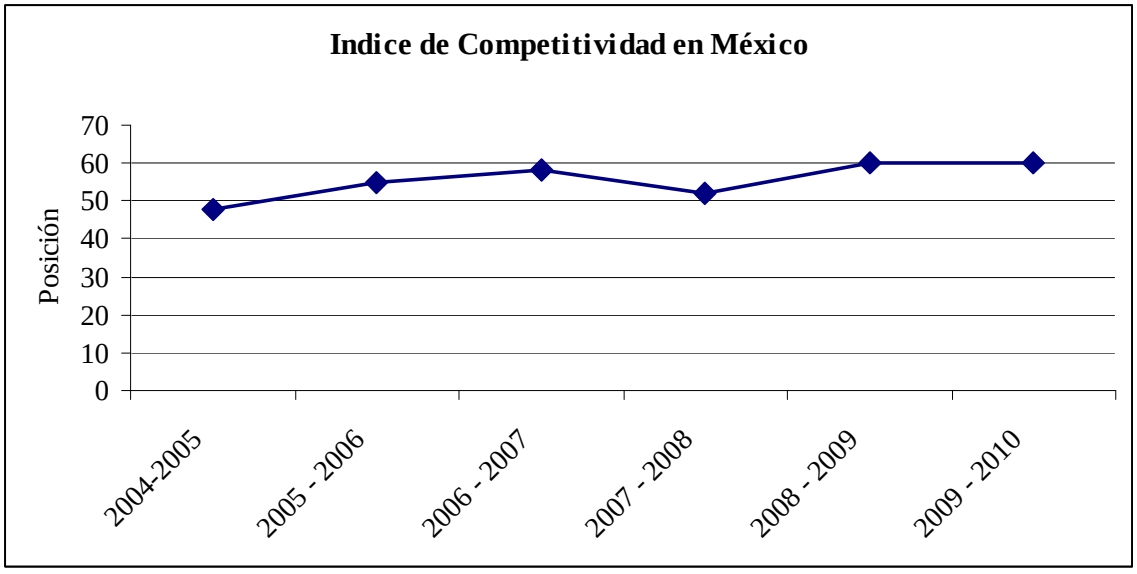
Tendencias de la seguridad informática en México

Para comprender cuáles son las tendencias en nuestro país, es conveniente conocer la situación actual que enfrenta México en materia de seguridad informática, por ello es conveniente analizar una serie de factores que influyen en el desarrollo de ésta, por lo que se vuelve indispensable analizar los diferentes sectores que se rigen en nuestro país, como por ejemplo, la educación, la salud, la seguridad y la infraestructura, identificando el tipo de tecnología que utilizan así como el nivel de concientización que existe en las organizaciones sobre la importancia de la seguridad informática y las políticas de seguridad que éstas manejan.

Si bien es cierto, las Tecnologías de Información y Comunicación (TIC) son un enorme potencial para mejorar la productividad del país, por lo tanto para el caso particular de este trabajo de investigación es conveniente analizar el índice de competitividad en el que se encuentra México, para así tomar medidas que ayuden a solucionar los puntos débiles que éste presenta; por lo que se vuelve indispensable que en nuestro país se haga un uso eficiente de los recursos públicos, como en los sectores: educativo, salud, seguridad, combate a la pobreza, infraestructura y gobierno electrónico (e-gobierno), para así lograr ser un país altamente competitivo.

3.1 Antecedentes

Durante los últimos años México ha venido perdiendo competitividad, (según datos emitidos por el Foro Económico Mundial) esto es, que el país deja de ser atractivo para los inversionistas nacionales e internacionales, teniendo como consecuencia que las empresas dejen de producir por no tener el nivel de competencia adecuado que los mercados requieren, es decir, el trabajo que se podría desarrollar en el país migraría hacia otros países. En la gráfica 3.1 se puede observar el comportamiento de México en el período comprendido del año 2004 al año 2009.



Gráfica 3.1 Índice de competitividad en México (2004-2005 / 2009-2010)

Desafortunadamente México se ha mantenido en un nivel de competitividad muy bajo con respecto a los países del mundo, ya que en los dos últimos años (2008 y 2009) se ha mantenido en el lugar 60 de 134 países del "ranking de competitividad" elaborado por el Foro Económico Global en su informe 2009-2010.[29]

Este informe señala que los principales problemas para realizar negocios están basados en la ineficiencia de la burocracia, la corrupción, el crimen, el robo y el acceso al financiamiento, entre otros.

[29] http://72.52.156.225/Estudio.aspx?Estudio=indice-competitividad

Lo que respecta a Latinoamérica, Chile ocupa el primer lugar ya que se ubica en el sitio 30, seguido de Puerto Rico en el sitio 42, Costa Rica en el sitio 55, Brasil en el sitio 56, Panamá en el sitio 59 y México ocupando el sexto lugar.

Los países que ocupan los primeros lugares según los datos emitidos en este foro son; Suiza, Estados Unidos, Singapur, Suecia y Dinamarca. Suiza desplazó a Estados Unidos por su capacidad de innovación así como de su sofisticada cultura de negocios, también por sus servicios públicos efectivos y su excelente infraestructura.

Cabe destacar que las Tecnologías de la Información y Comunicaciones (TIC) son una de las herramientas más eficientes para detonar la productividad en las empresas, porque permite un gran avance en la eficiencia de los mercados de producción e impacta en la vida de los ciudadanos mejorando el acceso, la eficiencia y la eficacia de los servicios públicos, transformando la comunicación entre la ciudadanía y gobierno, haciéndola directa, personal e inmediata.

3.2 Situación actual

La situación actual de México en los principales sectores, que son la base para tener un mayor índice de competitividad es delicada, por lo que a continuación se analizará un informe emitido por el Foro Económico Mundial sobre la situación actual de las TIC, así mismo, se dará a conocer un estudio sobre la Tercera Encuesta Nacional sobre Seguridad Informática en México. Todo ello con la finalidad de entender la situación en la que se encuentra nuestro país e identificar la problemática que existe.

A continuación se analizará la situación actual de las TIC en los diferentes sectores y la problemática que enfrentan actualmente:

a) **Las TIC en la educación:** Según datos emitidos por la Organización para la Cooperación y el Desarrollo Económico (OCDE) en su informe correspondiente al

> año 2009[30], señala que en México la esperanza de vida escolar por alumno es de 14.2 años, a diferencia de Finlandia y Suecia que supera los 20 años de esperanza de vida escolar. En México el índice de población que ha alcanzado estudios superiores entre 25 y 34 años es del 19%, lo que implica que aún se encuentra por debajo del promedio marcado por la OCDE que es del 39%, es decir, se tiene un déficit de -50%.

Por lo antes mencionado es conveniente que se realicen una serie de propuestas que ayuden a mejorar la calidad educativa de nuestro país, para así, lograr que los futuros profesionistas tengan, junto con el apoyo del gobierno, un nivel de conocimientos acorde a las necesidades que el país demanda para que pueda estar dentro de los principales países con un índice de competitividad alto y así mejorar su productividad.

Por otro lado, la Asociación Mexicana de la Industria de Tecnologías de Información (AMITI) en su informe "México Visión 2020"[31] publicado en el año 2006, menciona que uno de los principales problemas en nuestro país en materia de educación es la alta deserción de la educación media y media superior así como la baja calidad educativa, la desigualdad y el enorme rezago educativo de la población económicamente activa. Para combatir estos problemas las TIC son una de las herramientas más poderosas que están disponibles, ya que permiten llevar más educación a prácticamente cualquier lugar del país a un menor costo dándole la oportunidad al alumno a cursar materias a su propio ritmo.

La evidencia al respecto es clara, como lo muestran las experiencias de Corea, Chile o Finlandia, pero inclusive en México, donde programas piloto como el de "Secundaria Siglo 21" y el uso de Enciclomedia (Ver Figura 3.1), que entre otros propósitos enseña inglés, han dado frutos muy valiosos.

[30] http://www.educacion.es/dctm/ministerio/horizontales/prensa/documentos/2009/informe-espanol-panorama-educacion-ocde.pdf?documentId=0901e72b8007cd90
[31] http://www.cysp.com.mx/Ima/Amiti/Documentos%20Descargables/Doc_PP_vision_Mexico_2020.pdf

Figura 3.1 Enciclomedia

Uno de los principales problemas para el uso de las TIC es que la conectividad de las escuelas públicas es muy baja, aun frente a otros países latinoamericanos como Brasil o Chile. Se estima que en nuestro país menos del 12% de las primarias y secundarias tienen computadoras conectadas a Internet y aún menos tienen cursos y profesores capacitados para enseñar TIC. Mientras tanto, en Chile, las proporciones son cercanas al 70% y en Brasil se encuentran sobre un 40%.

Por lo tanto, los principales problemas para emplear las TIC en la educación están en la conectividad de los centros educativos del país y la falta de contenidos educativos que aprovechen la red para educar a cualquier mexicano, sin importar su edad, por ello, el uso de las TIC en la educación ha probado mejorar el acceso y la calidad de la educación en México. Pero la experiencia internacional muestra que las TIC han sido determinantes para cambiar el modelo pedagógico de la educación, de un modelo de memorización a uno basado en la investigación.

b) Las TIC en la salud: Una de las áreas más prometedoras para el uso de las TIC en México es el sector de la salud pública, ya que sin una población sana es difícil hablar de competitividad. La situación actual de México, en este sector, es de especial relevancia porque la población envejece a tasas de 4% anual y las principales causas de muerte se han convertido recientemente en enfermedades crónicas, muy caras de tratar. Además los servicios de salud pública sufren dos grandes problemas: baja calidad e insuficiente cobertura. Aunque ya se ha comenzado a trabajar en materia de salud, aún y a pesar de los grandes avances, los subsistemas apenas están iniciándose en el aprovechamiento integral de la tecnología.

La telemedicina (ver Figura 3.2), por ejemplo, ha permitido acercar los servicios de salud a lugares remotos con un costo mínimo, además de elevar la calidad de los servicios. El problema más importante a vencer para adoptar las TIC en este sector es el de conectividad e interoperabilidad de los distintos sistemas de salud (IMSSS, ISSSTE y SSA). En la actualidad, ésta es escasa en algunos lugares y por lo general con un costo elevado, por lo que se requiere un plan para conectar gradualmente los centros de salud con banda ancha, junto con la participación del sector privado.

Figura 3.2 Telemedicina

c) **Las TIC en la seguridad:** Actualmente 4 de cada 5 mexicanos cambian sus actividades por las condiciones de inseguridad que vive el país, ya que México tiene una de las probabilidades de condena más bajas del mundo: sólo 1 de cada 100 delitos que se cometen culminan en un castigo para el delincuente. La raíz del problema de la inseguridad radica en las grandes ineficiencias que hay en el sistema de procuración de justicia, por lo tanto, la falta de confianza que esto genera de las autoridades agrava aún más el problema, ya que el sistema actual es tan escaso que se ha entrado en un círculo vicioso en el cual los ciudadanos ya no denuncian delitos, con lo que, paradójicamente, reduce la presión sobre las autoridades para cambiar.

Las TIC han mostrado ser una herramienta clave para mejorar los sistemas de procuración de justicia en el mundo. Por un lado, hacen más eficiente la prevención y combate al delito y por otro, hacen expedito y transparente el funcionamiento del resto de la cadena de procuración de justicia: tribunales, juzgados y ministerios públicos.

Aún falta mucho por hacer, pues México apenas está comenzando a aprovechar las TIC dentro de su sistema de procuración de justicia. Cabe mencionar que, las reformas al sistema de justicia penal que están adoptando y promoviendo algunos estados como Chihuahua, Nuevo León y Oaxaca contemplan la creación de policías investigadoras y el mayor uso de TIC en todo el sistema.

d) **Las TIC en la seguridad nacional:** A partir de los cambios ocasionados por los ataques del 11 de Septiembre, Norteamérica ha implementado un nuevo programa de seguridad para homologar las Tecnologías de Información y Comunicaciones y asegurar las fronteras entre los tres países de América del Norte con objeto de combatir el terrorismo.

México firmó compromisos para adoptar estándares de TIC que permitan tener un mayor control e información sobre el cruce de personas y mercancías en la región. Esto permitirá tener importantes efectos colaterales, sobre todo en el sistema de seguridad.

e) **Las TIC en el combate a la pobreza:** La pobreza es uno de los principales problemas del país, puesto que cerca de 50 millones de mexicanos viven en condiciones muy precarias. Aunque las TIC todavía no alcanzan más que a una mínima proporción de esta población, su uso se ha hecho común, principalmente en la planeación de políticas sociales. Por ejemplo, ya está casi totalmente integrado un padrón único de beneficiarios sociales que permite eliminar duplicaciones y llevar programas sociales a la medida, proporcionando los servicios que realmente requiere la población más marginada.

El siguiente paso es integrar a la población en pobreza a la economía a través del uso de la tecnología, permitiéndoles:

- Tener acceso a la información de precios de productos, principalmente agrícolas.
- Utilizar el correo electrónico para mantener contacto con familiares y vincular cadenas productivas.
- Acceder a la información de los programas de gobierno (servicios de salud, educación y financiamiento entre otros).

Conforme se vayan obteniendo estos logros, se podrán incrementar las actividades que puedan realizar, logrando como objetivo principal, combatir la pobreza.

f) **Las TIC en la infraestructura:** Una ventaja competitiva indiscutible que tiene México es su colindancia con los Estados Unidos de América (el primer mercado del mundo) lo que implica mantener recorridos menores en tiempo y distancia, por lo tanto, los costos de transporte significativamente son más bajos que los de sus principales competidores.

Algunos de los principales problemas que originan estos costos pueden y deben solucionarse mediante la adopción de las TIC. Por ejemplo, la posibilidad de contar con información en tiempo real sobre las vías de comunicación no sólo permite un mejor uso de la infraestructura y un menor peaje en puertos, carreteras y ferrocarriles, sino también un mejor mantenimiento de esta valiosa infraestructura. Además, el uso de tecnología ya ha

probado ser de suma importancia en el cruce de mercancía dentro de las aduanas del país, por lo que el esfuerzo por digitalizar toda su operación debe continuar.

g) **Gobierno en línea**: La capacidad de poner cualquier trámite del gobierno en línea de forma fácil y expedita es uno de los principales motores para que los gobiernos en el mundo utilicen las TIC de manera intensiva y mejoren su comunicación con la ciudadanía.

En este sentido, México no ha sido la excepción y ha utilizado las TIC para comunicarse con la ciudadanía y proveer servicios en línea, como el pago de impuestos, las compras del gobierno, servicios de telemedicina, citas para obtener pasaportes y muchos más a los que actualmente acceden los ciudadanos de forma gratuita y desde cualquier lugar. Existen importantes barreras regulatorias, presupuestales y un grave problema de interoperabilidad, así como una brecha digital a vencer. Ante ello, es indudable que el principal reto para el próximo gobierno, en lo referente al gobierno electrónico, es la institucionalización y consolidación del mismo.

Tercer Encuesta Nacional sobre Seguridad Informática en México 2009

Esta encuesta fue realizada por el Departamento de Sistemas e Industrial de la Universidad del Valle de Atemajac (UNIVA), Campus Guadalajara – México en colaboración con la Asociación Colombiana de Ingenieros en Sistemas (ACIS), también se integró el Centro de Atención de incidentes de Seguridad y Telecomunicaciones (ANTEL) de Uruguay[32].

En este informe se analizaron datos proporcionados por empresas mexicanas que respondieron a una encuesta con 32 rubros clasificados en las siguientes categorías: Demografía, Presupuesto, Fallas de Seguridad, Herramientas y Prácticas de Seguridad Informática, Políticas de Seguridad y Capital Intelectual. Cabe destacar que se tomaron en cuenta datos comprendidos del período 2007 al 2009.

[32] http://www.acis.org.co/fileadmin/Revista_110/05investigacion2.pdf

Análisis de Categorías

Demografía: El propósito de esta categoría es identificar los sectores de participación y el cargo de quién tiene asignado la responsabilidad de la seguridad informática en la organización.

En la tabla 1 se puede observar a cargo de quién están las tareas de gestión de la seguridad, coincidiendo con años anteriores, la tarea es para el personal de tecnologías de información, aunque un 25% señaló que aún no tiene definido un puesto en particular para esta actividad.

Tabla 3.1 Responsabilidad de la seguridad informática

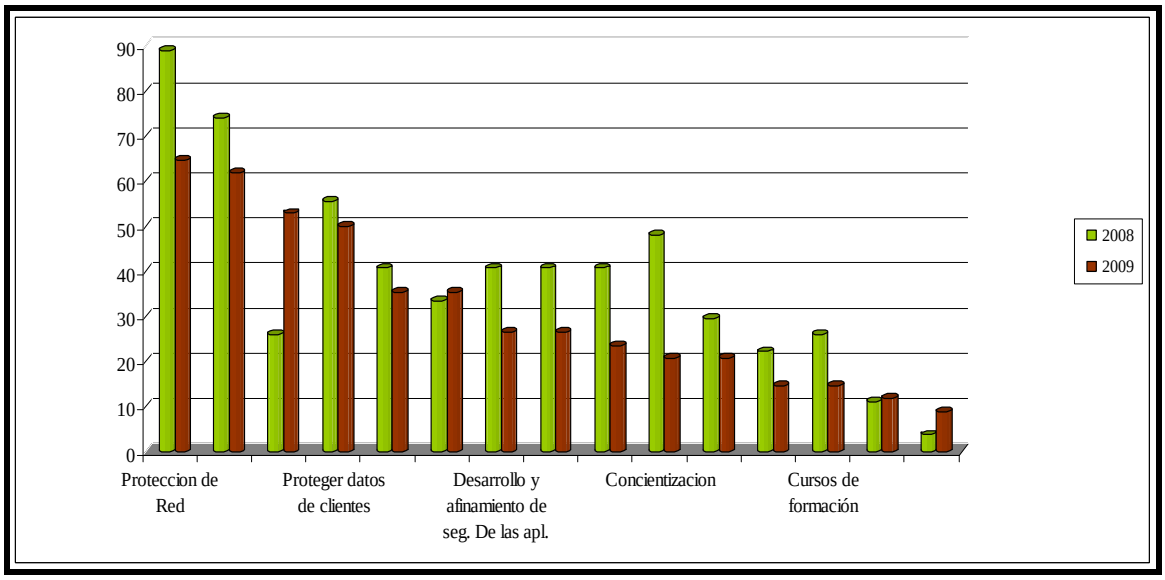
Responsabilidad de la SI	2007	2008	2009
Director Departamento de Sistemas / Tecnología	38.9%	29%	31.25%
No se tiene especificado formalmente	14.8%	26%	25%
Director de SI	11.1%	3%	**20.83%**
Auditoría Interna	1.9%	6%	10.41%
Otra (Por favor especifique)	14.8%	3%	8.33%
Gerente de Operaciones	0%	3%	4.16%
Gerente Ejecutivo	1.9%	29%	0%
Gerente de Finanzas	0%	0%	0%

Cabe destacar que existe un incremento sobre la presencia del cargo de Director de Seguridad Informática con un 20.83%, lo que significa que la información está siendo considerada como un valioso activo para las organizaciones, por lo tanto, vale la pena seguir realizando inversiones en su estructura organizacional.

Presupuesto: El propósito de esta categoría es revisar el presupuesto financiero destinado por las organizaciones a la gestión de la seguridad informática.

La distribución de presupuestos para cubrir las necesidades de todas las áreas de una organización se ha ido consolidando, en particular para la gestión de la seguridad informática.

En la gráfica 3.2 se muestra cómo es que únicamente en dos casos la distribución de presupuesto tiende a la baja durante el 2009 en relación con el año anterior, alguna de las causas puede ser la crisis económica global. Por otra parte, los aspectos que resaltan considerablemente son: pago a los asesores de seguridad informática con un incremento del 52.9% contra el 25.9% del 2008 y los cursos de especialización con un aumento del 2%.



Gráfica 3.2 Distribución del presupuesto para la GSI

Esto significa que en las organizaciones hay un mayor interés por contar con personal más capacitado en materia de seguridad informática, así como en la apertura para recibir orientación sobre cómo mejorar los procesos de la seguridad informática.

Fallas de Seguridad: El propósito de esta categoría es revisar los tipos de ataques e incidentes de seguridad más frecuentes, así como la manera en la cual las empresas se enteran sobre ellas y a quiénes notifican. También se busca conocer las causas por las cuales no se denuncian los incidentes y si se conoce lo suficiente sobre la evidencia digital.
En primera instancia se evaluó la percepción que se tiene en relación al valor de la información, considerando ésta como un activo, el cual el 12.5% de los participantes (menos de la mitad) consideran que la información es un activo más a proteger.

Otro dato que resulta interesante es la disminución en la identificación de intrusiones, que en buena medida puede obedecer a los niveles de seguridad que se han ido estableciendo al crecimiento en cultura informática de la sociedad. En la tabla 3.2 se aprecia una baja considerable en situaciones críticas, por ejemplo, para el caso de los virus detectados en el año 2008 representaron el 88.9% y para el año 2009 se manifestaron un 50%.

Tabla 3.2 Casos de violaciones a la seguridad informática

Casos de Violaciones	2008	2009
Virus	88.9%	50%
Instalación de software no autorizado	50%	31.25%
Accesos no autorizados al web	44.4%	27.08%
Manipulación de aplicaciones de software	11.1%	10.41%
Pérdida de información	22.2%	12.50%
Negación del servicio	11.1%	10.41%
Phishing	22.2%	10.41%
Otro: Fuga de información	5.6%	10.41%
Robo de datos	11.1%	8.33%
Monitoreo no autorizado del tráfico	5.6%	4.16%
Caballos de Troya	44.4%	6.25%
Ninguno	5.6%	4.16%
Pérdida de integridad	5.6%	4.16%
Suplantación de identidad	16.7%	4.2%
Pharming	5.6%	5.6%
Fraude	5.6%	2.08%

Por lo tanto, se aprecia de la tabla anterior que en la mayoría de los casos se han disminuido los diversos incidentes a los que se está expuesto, logrando así generar más confianza en las empresas para que inviertan en seguridad.

En cuanto a la notificación de denuncias, en la tabla 3.3, se muestran los diversos medios que existen para denunciar los incidentes.

Tabla 3.3 Entidad de notificación de denuncia

Entidad de notificación de denuncia	2007	2008	2009
Equipo de atención de incidentes	48%	44.4%	22.9%
Ninguno: No se denuncian	40%	38.9%	22.9%
Asesor legal	8%	16.7%	12.5%
Autoridades locales/regionales	4%	16.7%	10.4%
Autoridades nacionales	0%	0%	8.3%

De la tabla anterior se puede observar que la tendencia es no denunciar, sin embargo, esta situación puede modificarse si las autoridades nacionales van realizando acciones que, ante los ojos de los usuarios, los presenten como instancia competente para la resolución y control de delitos informáticos ya que desafortunadamente se ha optado por no denunciar debido a que no sucede nada o bien, se desconoce ante quien denunciar.

Herramientas y prácticas de seguridad informática: El propósito de esta categoría es identificar la frecuencia de pruebas de la seguridad, así como las herramientas y mecanismos para mantenerse actualizado sobre las posibles vulnerabilidades de los sistemas de información. A continuación se muestra en la tabla 3.4, la frecuencia de pruebas de seguridad en las organizaciones.

Tabla 3.4 Frecuencia de pruebas de seguridad en la organización

Frecuencia de pruebas de seguridad en la organización	2007	2008	2009
Una al año	25%	21.7%	12.5%
Entre 2 y 4 al año	27.5%	21.7%	18.75%
Mas de 4 al año	20%	21.7%	8.33%
Ninguna	27.5%	34.8%	16.66%
Sin respuesta			43.75%

De la tabla 3.4 se puede apreciar que la frecuencia de pruebas de seguridad es más activa, esto pudiera ser a que se cuenta con profesionales especializados dentro de la empresa, así como del aumento del nivel de conciencia en los usuarios sobre el cuidado de la información.

Complementando lo anterior en la tabla 3.5 se muestran los mecanismos utilizados para la protección de los sistemas de información. La herramienta más utilizada es el antivirus, seguido de las contraseñas y los respectivos firewall's, lo que significa que en las organizaciones se está invirtiendo poco a poco en seguridad informática, logrando así proteger sus activos. Se espera que se siga incrementando el uso de estas herramientas ya que cada día surge un nuevo tipo de amenaza y hay que evitar en la medida de lo posible que sean victimas de los ciber-delincuentes.

Tabla 3.5 Mecanismos utilizados para la protección de los sistemas de información

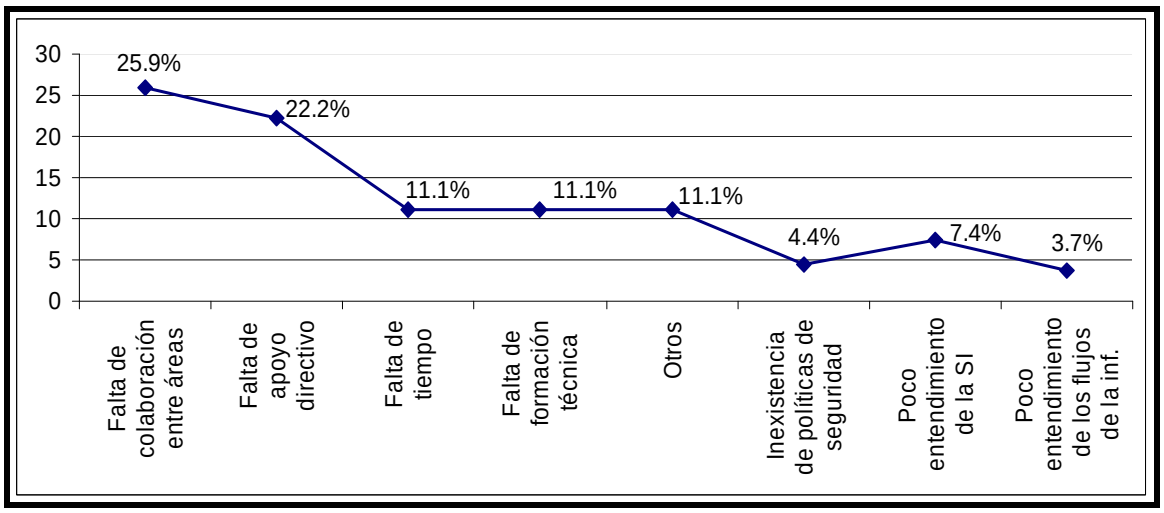
Mecanismos utilizados para protección de los SI	2007	2008	2009
Antivirus	70.4%	91.3%	50%
Contraseñas	68.5%	87%	47.91%
Firewalls Software	59.3%	65.2%	39.58%
Firewalls Hardware	44.4%	56.5%	35.41%
VPN/IPSec	40.7%	60.9%	33.33%
Cifrado de datos	50%	52.2%	31.25%
Sistemas de detección de intrusos – IDS	25.9%	17.4%	29.16%
Filtro de paquetes	31.5%	30.4%	25%
Biométricos (huella digital, iris, etc.)	9.3%	26.1%	25%
Administración de logs	0%	34.8%	22.91%
Firmas digitales / certificados digitales	31.5%	30.4%	22.91%
Web Application Firewalls	0%	43.5%	20.83%
Proxies	37%	39.1%	20.83%
Monitoreo 7x24	29.6%	30.4%	20.83%
Sistemas de prevención de intrusos - IPS	14.8%	30.4%	18.75%
Smart Cards	9.3%	26.1%	14.58%
Herramientas de validación de cumplimiento con regulaciones internacionales			6.25%
ADS (Anomaly detection systems)	13%	13%	4.16%

Políticas de seguridad: El propósito de esta categoría es conocer el estado que conserva la implementación de políticas de seguridad en la organización, considerando su aplicación, estándares y la colaboración con autoridades nacionales e internacionales.

Después de haber analizado las categorías descritas anteriormente, se puede decir, que existe un interés en las organizaciones por garantizar la seguridad de los recursos informáticos, disponiendo para ello recursos financieros y personal de apoyo. Sin embargo actualmente sólo el 20.8% dice contar con políticas de seguridad formales, el 14.6% indica estar en proceso de desarrollo y el 64.4% de los participantes no han iniciado un diseño o se abstuvieron en responder.

Otro punto de especial análisis es la adecuada Gestión de la Seguridad Informática. Existen diversas razones para que ésta pueda operar, destacando la falta de cooperación entre diversas áreas, la falta de apoyo directivo, la falta de tiempo, la falta de formación técnica, la inexistencia de políticas de seguridad, el poco entendimiento de la seguridad informática

y el poco entendimiento de los flujos de la información. En la gráfica 3.3 se muestran los principales obstáculos para lograr una adecuada gestión de la Seguridad Informática.



Gráfica 3.3 Obstáculos para lograr una adecuada gestión de la SI

Desafortunadamente la falta de colaboración entre las áreas / departamentos y la falta de apoyo directivo figuran cómo los principales obstáculos en la Gestión de la Seguridad Informática; por ello se sugiere, que el personal que labora en las organizaciones esté más informada y sobre todo que reflexionen sobre la problemática existente para que ayuden a disminuir los diversos obstáculos que se presenten.

Capital Intelectual: El propósito de esta categoría es conocer la demanda del profesional en seguridad informática y la importancia que tiene para las organizaciones las certificaciones en este tema.

Las empresas consideran la presencia del profesional en materia de seguridad informática, y señala que con dos años o más de experiencia, son necesarios para desempeñar cargos relacionados con el tema de la SI.

En relación a las certificaciones que actualmente tiene el personal del área de TI, se puede observar en la tabla 3.6 que existe una considerable baja en relación al 2007 y 2008.

Tabla 3.6 Clasificaciones de personal, dedicado al tema de la SI

Clasificaciones de personal dedicado al tema de la SI	2007	2008	2009
Ninguna	44.2%	39.1%	39.6%
CISSP (Certified Information Systems Security Professional)	11.5%	30.4%	10.4%
CISA (Certified Information Systems Auditor)	13.5%	26.1%	6.3%
CISM (Certified Information Security Manager)	15.4%	30.4%	6.3%
CFE (Certified Fraud Examiner)	3.8%	8.7%	0%
CIFI (Certified Information Forensic Investigator)	3.8%	8.7%	0%
CIA (Certified Internal Auditor)	7.7%	13%	2.1%
SECURITY+	0%	13%	4.2%
Otras (CCSP, CEH, OPST, OPSA, CCP)	11.5%	34.8%	8.3%
Sin Respuesta			22.9%

Se puede observar que la certificación que más figuró en el último año fue la CISSP con un 10.4%, aunque hay personal certificado, no debe quitarse la vista del 39.6% que indica que ningún profesional lo haya realizado.

Un dato importante que se señala en esta encuesta es el hecho de la poca importancia que tiene para las organizaciones, que el personal esté certificado; para el año 2009 aumentó, ya que para todos los tipos citados, la respuesta “no es importante” se ubica por encima de los resultados de valoración “muy importante”. Por lo que en esta categoría se tiene una fuerte área de oportunidad.

El impacto que ejercen las tecnologías de la información es muy fuerte ya que es lo más representativo para el desarrollo de las organizaciones, los nuevos modelos de administración y planeación estratégica, las incluyen ya no sólo como el medio mediante el cual se podrán ingresar datos, procesarlos y generar informes, ahora son un conducto a través del cual se puede generar valor en la organización pasando de una entidad que se

deja llevar con el flujo de la economía a una que de manera estratégica se convierta en insumo para lograr el desarrollo de las naciones, favoreciendo su propio crecimiento.

Los resultados que genera esta investigación, hablan del interés por considerar a la seguridad de la información como una estrategia que ayude al desarrollo organizacional, reflejándose en primer instancia por el reconocimiento del valor de la información, en la incorporación de políticas de control, en la integración de personal especializado en el tema dentro de la estructura organizacional, realizando inversión financiera; sin embargo, debe reconocerse, que México aún tiene un camino por recorrer en el terreno de la seguridad, tarea que sólo podrá despegar cuando todos los miembros de las organizaciones consideren a las TIC y a la información como columna y base que sostengan el proceso de planeación operativa y estratégica.
Por lo tanto se concluye que la inversión en el rubro de la seguridad de la información es una estrategia que podría mejorar el desempeño de las organizaciones.

3.3 Tendencias

Según el Instituto Mexicano para la Competitividad (IMCO) espera, a largo plazo, promover la adopción de las TIC para lo cual es indispensable generar consensos que den continuidad a las mismas. Por ello se propone para el año 2020:

- Mantener una República totalmente conectada mediante el uso de las TIC.
- Que México sea un país donde los mexicanos participen en la toma de decisiones económicas, políticas, sociales y culturales por medio del uso de las TIC.
- Tener empresas y gobiernos innovadores, eficientes e inteligentes que desplieguen sus capacidades a través del uso intensivo de las TIC.
- Posicionar a México en el lugar 20 a nivel mundial apoyándose en las TIC.

La mejora en la competitividad ubicaría a México en una posición similar a la que tienen hoy países como Chile o Portugal. Aunque la meta es grande, pero estimaciones realizadas

por el IMCO muestran que el 70% del cambio se concentra en 3 principales factores de competitividad, que son:

- Tener gobiernos eficaces y eficientes.
- Aprovechar productivamente las relaciones internacionales del país.
- Proveer un sistema de derecho que sea confiable y objetivo que brinde seguridad a las empresas y a las personas.

Estos 3 factores tienen dos ventajas:

1. Ninguno de ellos es particularmente polémico, es decir, cabe fácilmente dentro de la agenda política de los principales partidos políticos.
2. Todos estos factores dependen en buena medida de la provisión eficiente de servicios por parte del gobierno federal y los gobiernos locales.

Por lo tanto, las estimaciones del IMCO muestran que con sólo mejorar la eficiencia de los gobiernos se puede alcanzar cerca del 30% del aumento total que provendría de tener índices más altos de competitividad. Por ello, la adopción de las TIC por parte del gobierno será determinante en la mejora de la competitividad del país, sin que ello signifique hacer a un lado otros temas, como son las reformas estructurales.

La visión 2020 se construyó a partir del estudio de las mejores prácticas en el mundo. Se organizó en torno a cuatro segmentos económicos que usan las TIC y son:

1. La ciudadanía

Se espera que para el año 2020 la participación de los mexicanos en la vida económica, política y social del país se incrementará notablemente gracias al uso y aprovechamiento de las TIC, lo que posibilitará a los ciudadanos no sólo estar en contacto con los gobernantes y ser parte del proceso de toma de decisiones, sino también con el resto del mundo.

Para lograrlo, es necesario cerrar la brecha digital, lo cual significa proveer la conectividad necesaria y alfabetizar digitalmente a la población para que pueda hacer uso de la

tecnología, lo que implica cambios profundos dentro del sistema escolarizado, la incorporación de materias de tecnología en la educación básica y la creación de nuevos contenidos para toda la población como por ejemplo, asegurar que los jóvenes mexicanos dentro de la educación básica y media aprendan inglés.

Para ese año se pretende que toda la población mexicana tenga acceso digital de banda ancha desde cuando menos un punto físico, ya sea el hogar, la escuela, el trabajo, algún centro comunitario digital o su aparato personal de telecomunicación celular.

Algunas de las implicaciones del uso de las TIC por la población son:

- Contar con trabajadores "móviles" conectados desde cualquier lugar. Por ejemplo, para el año 2020 los trabajadores podrán hacer traspasos de datos, video, voz y hasta dinero, desde su celular o computadora portátil, lo que les permitirá trabajar desde cualquier lugar y en cualquier momento.
- Una población educada que podrá cursar desde la educación básica hasta postgrados en línea, respaldada por contenidos educativos de altísima calidad, exámenes de acreditación y asesorías que le permitirán adquirir nuevos conocimientos en cualquier lugar y a cualquier hora.
- Ciudades integradas mediante redes de acceso a Internet de banda ancha.

Todo lo anterior mencionado permitirá reducir las desigualdades económicas de la población, al contar con mayor educación, información y un diálogo personal y continuo con las autoridades.

2. Las empresas

Para el año 2020 México habrá evolucionado de ser un país cuya economía se concentra en la producción de manufacturas basadas en mano de obra barata, hacia uno que produce bienes y servicios de mayor valor agregado, es decir, el país se moverá de lo que se conoce como vieja economía hacia una nueva economía.

La industria mexicana en el 2020 se compondrá por aquellos sectores que se han posicionado en el mercado internacional y que continuarán haciéndolo como son: electrónica, automotriz, manufacturas avanzadas y agroindustria, entre otros, y por otro lado, para ese mismo año, habrá nuevos sectores que hoy muestran un gran potencial, pero que requieren de nuevas tecnologías y modelos de desarrollo para posicionarse dentro del mercado global, como: petroquímica, turismo, logística, TIC, contenidos en idioma español, industria aeroespacial y subcontratación de procesos de negocios y de transformación de negocios.

Las empresas mexicanas del futuro se apoyarán en las TIC para hacer más eficientes sus operaciones y reinventar sus propuestas de valor al mercado. La eficiencia de las operaciones se logrará utilizando las TIC para agilizar la logística de la cadena de producción y consolidar sus procesos e infraestructura. Por otro lado, la reinvención de sus propuestas avanzará en dos sentidos:

- El desarrollo de productos y servicios accesibles para las clases de bajos ingresos.
- La generación de bienes y servicios con un mayor valor agregado, mediante la personalización de la oferta a clases medias altas.

Así, las empresas serán inteligentes y podrán obtener mayor información sobre cada uno de sus clientes. Ello permitirá la “personalización masiva” que combina tanto las ventajas de la gran escala con las de atención personalizada.

La alta disponibilidad y el bajo costo de enlaces de banda ancha, el avance del software de gestión y sobre todo la necesidad de seguridad, administración y soporte continuo, harán cada vez más necesaria la tercerización de servicios. Por ello, la consolidación de infraestructura y procesos contratados a terceros para lograr economías de escala, será cada día más común.

En cuanto a logística, el uso de TIC permitirá mejorar la eficiencia de las empresas por dos vías:

1. Contar con mayor información en tiempo real sobre demanda y patrones de consumo de los productos de las empresas.

2. Mejorar considerablemente en la infraestructura de telecomunicaciones, carreteras, aeropuertos y demás, ya que se espera que el país se convierta en un *hub* logístico para el mercado norteamericano.

Las TIC permitirán integrar las cadenas productivas a través de redes impulsando la productividad de las micro y pequeñas empresas.

Actualmente existen muestras del potencial de dicha integración dentro de la industria cementera, donde las grandes compañías instalan los servicios e infraestructura digital necesaria para integrar a los pequeños proveedores dentro de su red, lo que aumenta la productividad de toda la línea de producción.

Por último, el uso intensivo del comercio electrónico y de transacciones electrónicas cambiará drásticamente la forma de operar de las empresas. Se espera que cerca del 70% del valor de las transacciones entre las principales industrias se realice a través de la red, tanto de compra y venta de mercancía, como de emisión de facturas y recibos electrónicos.

3. La industria

Para el año 2020 la industria de las TIC será una base para reforzar la competitividad de todas las industrias. Los escenarios para cada uno de sus principales segmentos son:

- Para el año 2020 el país habrá desarrollado una masa crítica de empresas nacionales proveedoras de productos y servicios digitales. México tiene la oportunidad de fortalecer operaciones de mayor valor agregado en las áreas de desarrollo, diseño y prueba de componentes encapsulados que se usan en industrias como la automotriz, electrónica, petroquímica y aeroespacial, incluyendo diseño, programación y prueba de circuitos.
- México se posicionará como nodo de abasto y distribución de equipos electrónicos hacia Norte y Centroamérica, complementándose con los productores asiáticos a través de ensamble de equipo y manufactura flexible.

- La integración de soluciones verticales es quizá el futuro de la industria de software. El potencial de México para esta industria es enorme debido al crecimiento esperado en el mercado nacional e internacional. Las principales ventajas competitivas de México para la exportación de estos servicios son:
- Similitud de huso horario, lenguaje y/o cultura, con el mercado norteamericano y latinoamericano.
- Lazos comerciales fuertes con el mercado norteamericano.
- Mejores y generalmente más económicos servicios de voz y datos debido a la cercanía geográfica.
- Menores costos de transporte.
- Un gran potencial en el sector salud, derivado del acceso a médicos a precios competitivos y al enorme mercado potencial debido al envejecimiento de la población mundial, que se apoyará en servicios de outsourcing (solicitud de apoyo externo que una compañía requiere para manejar algunas de sus operaciones, las cuales ocupan un tiempo valioso[33]).
- Un nuevo mercado con gran potencial para tecnología de telecomunicaciones y servicios administrados basados en tecnología IP. Sólo el 27% de las empresas en México conoce este servicio, se espera que para el 2020 las empresas grandes y medianas habrán dado el salto a esta tecnología a través de paquetes administrados de voz por parte de los fabricantes de software y equipo de telecomunicaciones.

La sinergia, entre la integración de circuitos y su digitalización, así como el predominio de Internet y de las redes inalámbricas, seguirá ampliando y profundizando la convergencia tecnológica, hasta que en el 2020 la interconexión sea universal.

El software como servicio descansará en una nueva arquitectura, conocida como "servicios web" los cuales permitirán acoplar recursos tecnológicos de entidades distintas y de diversa índole.

[33] http://www.soyentrepreneur.com/home/index.php?idNota=2771&p=nota

4. El gobierno

El uso y aprovechamiento de las TIC dentro del sector público es quizá el paso más importante para hacer mas eficientes y transparentes los servicios públicos, así como acercar los gobiernos a la ciudadanía. Por ello, en esta sección se analizan en primer lugar, las metas y el uso intensivo de las TIC en los principales servicios públicos. En segundo lugar se expone la importancia de las TIC como una nueva forma de comunicar al gobierno con la sociedad, así como a la sociedad misma.

Cabe destacar que en esta categoría, se analizaron con mayor detalle las tendencias en los sectores educativos, salud, seguridad, seguridad nacional, combate a la pobreza, infraestructura y e-gobierno, las cuales se describen a continuación:

a) Educación: Para el 2020 se espera que las TIC hayan transformado el sistema educativo mexicano por completo, de tal forma que los alumnos ya no memoricen la información, sino que investiguen y desarrollen su creatividad. Se espera que:

- Se haya eliminado el rezago educativo en la población económicamente activa por medio de programas de alfabetización digital.
- Que toda la educación esté en línea, desde la educación básica hasta postgrados.
- Que se encuentre operando un sistema de educación para toda la vida, con distintos cursos en línea.

Por ello, el primer reto a enfrentar es el de la falta de conectividad en las escuelas, éstas no deberán no sólo estar conectadas, sino contar con al menos una conexión de alta velocidad de 10Mbps como mínimo. También se requiere crear contenidos educativos que se basen en el uso de la red como una de sus principales fuentes de información y permitan el intercambio de experiencias con alumnos y profesores de todo el mundo.

Para el 2020 se espera que todos los salones de clase sean multimedia y los profesores sirvan como facilitadores del conocimiento que estará en línea, también, los alumnos, padres de familia, profesores y empresas tendrán mayor contacto a través de portales

educativos que permitirán un diálogo entre las partes para vincular la academia con el mundo productivo y mejorar la educación fuera y dentro de la escuela.

b) Salud: El uso de las TIC no sólo mejora la calidad de servicios de salud y su cobertura, sino que permite una provisión de nuevos servicios para prevenir riesgos de salud. Las consultas y recetas en línea y el monitoreo de pacientes desde sus hogares tiene alcances muy importantes. Existe una demanda de servicios de salud provistos a través de redes de información, hoy, 3 de cada 4 usuarios de Internet en el mundo, buscan información relacionada a salud cuando están en línea.

Por ello, para el 2020 los índices de prevención de salud en la población mexicana deberán haberse triplicado, sobre todo a través del monitoreo y consultas en línea de temas de salud. Para lograr esto, todos los mexicanos deberán contar con un expediente médico electrónico que incluya un organizador de salud que les permita saber las medicinas que han consumido y los síntomas que han presentado a lo largo de su vida. También el Sistema Nacional de Salud Pública en México deberá permitir consultas todos los días del año a cualquier hora, así como también el intercambio de información entre pacientes y médicos.

Para lograrlo, se requiere conectar los centros de salud por medio de banda ancha y lograr la interoperabilidad entre los sistemas del IMSS, ISSSTE y Secretaría de Salud, así como de las instituciones de salud privadas.

Lo anterior no es difícil de lograr, puesto que al ritmo que evoluciona la tecnología es indiscutible que en 2020 las consultas a distancia se harán en algunos casos desde teléfonos celulares y/o dispositivos móviles que permitirán por ejemplo, la transmisión de voz, datos, videos e información sobre ritmos cardiacos a un médico, que podrá revisarlos conforme al expediente médico electrónico del paciente y así diagnosticar y recomendar algún tratamiento.

c) Seguridad: Para el 2020 los avances descasarán en la tecnificación de policías y la adopción de las TIC dentro del sistema, aunque éstas ya figuran incipientemente como

en el caso de la integración de bases de datos de delincuentes y policías. Algunos otros servicios que también contribuirán de manera importante son:

- Bases de datos policíacas con información de vehículos y personas.
- La integración de información criminal de todas las dependencias públicas (federal, estatal y municipal) en un mismo padrón, lo que servirá como base para una nueva policía investigadora que empleará métodos científicos en sus labores.
- Sistemas de software avanzados que ya se utilizan en diversas partes del país, serán adoptados en todos los cuerpos de seguridad para integrar estadísticas del delito con información socioeconómica zonificada sobre planos geográficos digitalizados, lo que mejorará la prevención del delito.
- Sistemas de GPS en las patrullas, que permitan monitorear a los policías en labores donde la sociedad civil participará como observadora.
- Telefonía intercomunicada con todas las policías para intercambiar rápidamente voz y datos a través de celulares y/o dispositivos móviles.
- Número único de emergencia (parecido al 911 de EU), que funcionará para llamadas desde teléfonos fijos, celulares o de telefonía por Internet. Este servicio será monitoreado por la sociedad civil para evaluar las tendencias criminales, la ubicación de las zonas más conflictivas y la velocidad y eficacia de la atención de las fuerzas públicas y de rescate.
- Cámaras de televisión en los sitios de crimen potencial, entre otros.

d) Procuración de justicia: Para el 2020 todos los tribunales estarán digitalizados, lo cual permitirá que se puedan consultar las audiencias en línea mediante claves de acceso. En lugar de los largos expedientes en papel, se llevarán los expedientes electrónicamente e inclusive los juicios se podrán presenciar en línea. Los tribunales también deberán contar con portales donde los ciudadanos puedan obtener asesoría sobre cómo demandar y los pasos a seguir en una denuncia o juicio.

e) Seguridad nacional: Los acuerdos firmados en la Alianza para la Seguridad y la Prosperidad de América del Norte proporcionarán una nueva forma de comunicar al

país mediante el uso de las TIC con sus vecinos del norte. Por ello, la adopción de los estándares planteados es una oportunidad única para lograr una mayor integración con América del Norte, combatir el terrorismo y la propia delincuencia organizada en la frontera.

f) Combate a la pobreza: Para el 2020, México habrá reducido la pobreza de patrimonio en 30% y la pobreza alimentaria en 50%. Las TIC habrán contribuido a lograr dichas metas mediante la:

- Creación de programas más efectivos y focalizados de combate a la pobreza. Esto se logrará gracias al buen uso del padrón único de beneficiarios de política social que permitirá ofrecer programas a la medida para abatir la pobreza y modelos predictivos de evolución de la pobreza.
- Capacitación e información en línea a más población marginada sobre oportunidades de trabajo y servicios públicos disponibles.
- Información a la ciudadanía en general sobre las condiciones y necesidades de la población en pobreza.
- Capacitación e información en línea a más población marginada sobre oportunidades de trabajo y servicios públicos disponibles.
- Información a la ciudadanía en general sobre las condiciones y necesidades de la población en pobreza.
- Ampliación de programas sociales que se basen en el uso de las TIC, como celulares a pequeños productores que les permitan tener contacto con sus clientes finales y fijar precios, eliminando así a los intermediarios.

g) Infraestructura y otros servicios públicos: La posición geográfica de México, así como su capacidad para contar con mano de obra calificada y a precios competitivos, le permitirán posicionarse como un *hub* logístico para Norteamérica en el 2020. La columna vertebral del sistema de logística se basará en las Tecnologías de Información y Comunicaciones, por ejemplo, los chips de radiofrecuencia en contenedores permitirán saber el tipo de mercancías que se transportan, su temperatura y todos los cambios que habrá sufrido desde el embarque, permitiendo un control exacto a lo largo de toda la cadena logística.

El uso de las TIC también mejorará el manejo de infraestructura pública, como el agua y la energía, lo que permitirá un uso más transparente de los recursos e información sobre las pérdidas y flujos en cada parte de la red.

h) e-gobierno y las nuevas formas de comunicación entre la sociedad y el gobierno: la función del Estado no se reduce únicamente a transformar la comunicación entre los ciudadanos y los gobiernos, sino a garantizar las nuevas formas de comunicación entre la sociedad, esta será participativa en la toma de decisiones de sus comunidades, lo que implicará debates y votaciones en línea, también será una sociedad que comprará en línea; se espera que más del 70% del valor de las transacciones comerciales se realicen a través de la red. Para ello el gobierno deberá garantizar la seguridad en las transacciones electrónicas mediante:

- Infraestructura adecuada.
- Un sistema de correo y paquetería seguro y eficiente.
- Seguridad en medios de pago.
- Seguridad en el intercambio de información.
- Un marco jurídico que proteja a los consumidores de fraudes en línea.

El uso de las TIC está transformando la comunicación entre los gobiernos y la sociedad. Por ello, es fundamental entender la trayectoria que deberá seguir el país para permitir una comunicación cercana, personalizada y confidencial en la comunicación entre particulares.
La primera meta a desarrollar es una nueva forma de identificar con seguridad a todos los ciudadanos. Para el 2020 el registro de los mexicanos se realizará mediante la toma de huellas dactilares que estará disponible en una base de datos y en un *chip* que portará cada ciudadano en su cédula de identidad.

Por otro lado también habrá un sólo punto de contacto con el gobierno a través de una ventanilla única, como en el caso de Singapur, por ello, para el año 2020, las empresas y ciudadanos mexicanos podrán llevar a cabo cualquier trámite con gobierno en línea,

además de recibir correos y alertas vía celular sobre noticias parlamentarias, recordatorios de renovación de pasaporte u otros trámites.

Se concluye que la visión para el año 2020 no sólo implica el establecimiento de metas, sino también el planteamiento de las directrices que deberá seguir el país para cerrar las brechas digitales con el resto del mundo. Para ello es necesario construir una arquitectura institucional con una oficina que articule las acciones de adopción de las TIC al interior del gobierno. Por otro lado, si las autoridades no garantizan la confidencialidad y el resguardo de información personal en este nuevo esquema de intercambio de información, de poco servirá capacitar y conectar a la población, ya que no habrá confianza en los medios electrónicos. Por ello, para el 2020 existirá un Sistema Nacional de Administración de Información donde se almacenará la información y se garantizará la seguridad del intercambio de la misma entre gobiernos y dependencias.

Lo anterior permitirá que los mexicanos del 2020 participen en la toma de decisiones de sus comunidades, debatan y hasta posiblemente voten en línea. También permitirá erradicar el uso del papel y contar con un gobierno que se adapte a las nuevas necesidades de los ciudadanos. Sin embargo, no basta con tener una buena visión, se debe contar con una buena ejecución.

Es muy importante que se preste la atención adecuada a los sectores analizados anteriormente, ya que son la clave para que México pueda posicionarse como un país competitivo. Para lograrlo se requiere de mucho trabajo en equipo, hacer conciencia sobre la importancia del uso de las TIC así cómo de la protección de la información. Si la información no se protege, difícilmente se cumplirán los objetivos planteados para el futuro.

Invertir en seguridad informática hoy en día es una necesidad debido a la cantidad de dispositivos que existen para acceder a Internet, ya no solo hay que protegerse de las computadoras. Por ello es importante invertir recursos y capacitar a los usuarios para evitar en la medida de lo posible ser víctima de un ataque cibernético.

Capítulo 4
Análisis en materia de educación

Derivado del avance tecnológico que se ha venido dando en México, hoy en día las Tecnologías de la Información forman parte de nuestra vida cotidiana, por este motivo se hace un análisis de los planes de estudio de los diversos sectores educativos (educación Básica, Media Superior y Superior) en materia de seguridad informática, cuyo objetivo es identificar la situación en la que se encuentran y en base en ello, mejorar la calidad educativa de nuestro país.

Es importante que se lleve a cabo este análisis, ya que de esa manera se pueden generar propuestas para crear una cultura en seguridad informática y en tecnologías de la información.

4.1 Educación Básica (Primaria y Secundaria)

Para impulsar la seguridad informática en las escuelas públicas de educación básica, es necesario que se cuenten con las condiciones básicas e indispensables para establecer una conexión a Internet que sea gratuita para los alumnos, ya que es la base para impulsar a las actuales y futuras generaciones a una nueva cultura tecnológica. Todo esto con la finalidad de aprovechar al máximo los recursos tecnológicos y eficientar la enseñanza, para así eliminar el rezago educativo que existe en nuestro país. (Para conocer más sobre los planes de estudio ver los anexos 1 y 2).

Ante esta necesidad el gobierno del Distrito Federal puso en marcha el "Programa Integral de Conectividad Escolar 2008-2012" (Aula Digital) cuyo objetivo es asegurar que todas las escuelas públicas de la entidad tengan equipos de cómputo y conexión a Internet a fin de aprovechar estas herramientas para el mejor procesamiento de la información y las telecomunicaciones, para ampliar así sus capacidades y alcanzar mejores niveles de desempeño académico y mayores niveles de competitividad[39].

Específicamente consiste en instalar en 2,000 escuelas una "Aula Digital" con 25 computadoras, 26 mesas, 25 sillas, 1 equipo multifuncional y una red inalámbrica con servicio de Internet de banda ancha.

En términos generales el Programa se divide en 3 etapas:

1) **El Levantamiento (Diagnóstico) de las necesidades, escuela por escuela:** Consiste en la elaboración de un diagnóstico, escuela por escuela, de las condiciones en las que se encuentra el espacio disponible, las instalaciones eléctricas y las facilidades de mobiliario, a fin de ponerla a punto para recibir el equipo de cómputo y la conectividad.
2) **La capacitación de los instructores escolares:** Consiste en preparar a quienes en cada escuela se encargarán del aula TIC (del acrónimo de Tecnologías de la

[39]http://archivos.diputados.gob.mx/Comisiones/Especiales/Acceso_Digital/Presentaciones/Programadeconectividad_AulaDigital_GobDF.ppt

Información y la comunicación) a fin de que conozcan a fondo las características del equipo y los programas (software) que potencializarán su uso para fines académicos.

3) **La instalación del equipo de cómputo y la conectividad:** Consiste en instalar las redes de energía eléctrica y el mobiliario, así como los equipos de cómputo propiamente dichos y la conexión a Internet.

Para ello, se llevó a cabo un análisis, el cual consiste en mostrar las condiciones de conectividad de las escuelas públicas de educación básica del Distrito Federal y los datos que se obtuvieron se muestran en la tabla 4.1

Tabla 4.1 Conectividad de las escuelas públicas de educación básica del DF.

Categoría	Escuelas			Estudiantes		
	Sin conectividad	Con conectividad	Total	Sin acceso	Con acceso	Total
Primarias	2,120	178	2,298	701,000	61,087	762,087
Secundarias	36	935	971	15,000	402,357	417,357
Total	2,156	1,113	3,269	716,000	463,444	1,179,444

Fuentes: Principales Cifras del Ciclo Escolar 2006-2007 del Sistema Educativo de los Estados Unidos Mexicanos (Dirección General de Planeación y Programación, SEP); Programa Red Escolar/Instituto Latinoamericano de Comunicación Educativa 2008 ILCE).

Según estos datos, a finales del 2007 había 2,298 escuelas primarias públicas en el DF de las cuales alrededor de 2,120 (92%) no tenían conectividad y aunque los datos indican que en el nivel de secundarias el porcentaje de escuelas con conectividad era alto (96%), su situación es ya tan precaria, que en la mayoría de ellas habrá que hacer sustitución en los equipos y hacer una nueva conexión a Internet.

Considerando que el número promedio de estudiantes por escuela primaria es de 331, mientras que a nivel secundaria es de 429, se tiene que en las condiciones actuales, alrededor de 700 mil alumnos de educación primaria y más de 15 mil de secundaria se quedan al margen de las herramientas que mejorarían sensiblemente la calidad de su educación.

Con este programa, el Distrito Federal podrá estar en condiciones comparables con las de París y Lyon, con 100% de escuelas con conexión a Internet y en condiciones comparables

con las ciudades de Lyon o Madrid, en cuanto al número de alumnos por computadora (14) en escuelas de educación básica.

4.2 Educación Media

Para realizar una propuesta en este nivel educativo, se realizó un análisis general de los planes de estudio de las escuelas que pertenecen a la Universidad Nacional Autónoma de México (UNAM), como la Escuela Nacional Preparatoria (ENP) y el Colegio de Ciencias y Humanidades (CCH). Esto se realizó con la finalidad de identificar el nivel de conocimientos que tienen en materia de seguridad informática, es decir, identificar ¿Qué temas en materia de seguridad informática se les imparten a los alumnos?, ¿son adecuados los temas acorde al nivel educativo? y por último ¿Qué se propone para mejorar la calidad educativa en esta área? Así se presenta en primer lugar el plan de estudios de la ENP y posteriormente el del CCH.

4.2.1 Escuela Nacional Preparatoria (ENP)

En la tabla 4.2 se muestra el plan de estudios de la ENP que actualmente está en vigor.

Tabla 4.2 Planes y Programas de Estudio 1996

Asignaturas		
4to. Año	**5to. Año**	**6to. Año (Tronco Común)**
Matemáticas IV	Matemáticas V	Derecho
Física III	Química III	Literatura Mex. e Iberoam.
Lengua Española	Biología IV	Inglés VI
Historia Universal III	Educación para la Salud	Francés VI
Lógica	Historia de México II	Alemán II
Geografía	Etimologías Grecolatinas	Italiano II
Dibujo II	Leng.Extr. Ingles V	Inglés II
Leng. Extr. Ingles IV	Leng.Extr. Francés V	Francés II
Leng. Extr. Francés IV	Leng.Extr. Italiano I	Psicología
Educ. Estética-Artist. IV	Leng.Extr. Alemán I	Higiene Mental
Educación Física IV	Leng.Extr. Ingles I	Teatro VI
Orientación Educativa IV	Leng.Extr. Francés I	Música VI
Informática	Ética	Estadística y Prob.
	Educación Física V	

	Educ. Estética-Artist. V	
	Orientación Educativa V	
	Literatura Universal	
Área 1		
	Matemáticas VI	
	Dibujo Constructivo II	
	Física IV	
	Química IV	
	Biología V	
	Geología y Minerología	
	Físico-Química	
	Temas Selec. Matemáticas	
	Informática Aplicada a la Ciencia y la Industria	
	Cosmografía	

Fuente: http://dgenp.unam.mx/planesdeestudio/planesindex.html

Revisando el plan de estudios correspondiente a cada materia de tronco común en el cuarto año los alumnos cursan la asignatura de Informática el cual consta de 6 unidades:

1. Antecedentes de la Informática
2. Estructura física de una computadora
3. Procesamiento de textos
4. Estructura lógica de una computadora
5. Metodología de la Solución de problemas y programación
6. Software de aplicación y servicios de red

Se aprecia que desde que ingresan a la preparatoria se dan a conocer los elementos básicos de la computación. De manera particular se analiza el contenido de la unidad 6 el cual abarca los siguientes temas:

6.1 Ambientes gráficos

6.2 Hojas de cálculo

6.3 Manejadores de bases de datos

6.4 Editores gráficos

6.5 Servicios de red

4.2.2 Colegio de Ciencias y Humanidades (CCH)

En la tabla 4.3 se muestra el Plan de estudios del Colegio de Ciencias y Humanidades (CCH).

Tabla 4.3. Mapa curricular del plan de estudios del CCH

	Primer Semestre	Segundo Semestre
Asignaturas	Matemáticas I	Matemáticas II
	Taller de Cómputo I	**Taller de Cómputo II**
	Química I	Química II
	Historia Universal Moderna y Contemporánea I	Historia Universal Moderna y Contemporánea II
	Taller de Lect., Redacción e Iniciación a la Invest. Doc. I	Taller de Lect., Redacción e Iniciación a la Invest. Doc. II
	Inglés I / Francés I	Inglés II / Francés II
	Tercer Semestre	**Cuarto Semestre**
	Matemáticas III	Matemáticas IV
	Física I	Física II
	Biología I	Biología II
	Historia de México I	Historia de México II
	Taller de Lect., Redacción e Iniciación a la Invest. Doc. III	Taller de Lect., Redacción e Iniciación a la Invest. Doc. IV
	Inglés III / Francés III	Inglés IV / Francés IV
	Quinto Semestre	**Sexto Semestre**
	1ª Opción (Optativa) Oblig.	**1ª Opción (Optativa)**
	Cálculo I	Cálculo II
	Estadística I	Estadística II
	Cibernética y Computación I	**Cibernética y Computación II**
	2ª Opción (Optativa)	**2ª Opción (Optativa)**
	Biología III	Biología IV
	Física III	Física IV
	Química III	Química IV
	3ª Opción (Optativa)	**3ª Opción (Oblig.) Opt.**
	Filosofía I	Filosofía II
	Temas Selectos de Filosofía I	Temas Selectos de Filosofía II
	Administración I	Administración II
	Antropología I	Antropología II
	Ciencias de la Salud I	Ciencias de la Salud II
	Ciencias Políticas y Sociales I	Ciencias Políticas y Sociales II
	4ª Opción (Optativa)	**4ª Opción (Optativa)**
	Derecho I	Derecho II
	Economía I	Economía II
	Geografía I	Geografía II
	Psicología I	Psicología II
	Teoría de la Historia I	Teoría de la Historia II
	5ª Opción (Optativa)	**5ª Opción (Optativa)**
	Griego I	Griego II
	Latín I	Latín II

	Lectura y Análisis de Textos Literarios I	Lectura y Análisis de Textos Literarios II
	Taller de Comunicación I	Taller de Comunicación II
	Taller de Diseño Ambiental I	Taller de Diseño Ambiental II
	Taller de Expresión Gráfica I	Taller de Expresión Gráfica II

De la tabla anterior se observa que en el primero y segundo semestres se imparten las asignaturas de "Taller de Cómputo I y II" respectivamente. Se analizó el temario y se puede apreciar que consta de 10 unidades divididas en 2 semestres, es decir, en el primer semestre se imparte de la 1ª a la 5ª unidad y en el segundo semestre se imparte de la 6ª a la 10ª unidad. El contenido de este taller es el siguiente y se muestra en la tabla 4.4:

Tabla 4.4 Taller de Cómputo I y II

Taller de Cómputo I y II	
1. Historia de la computación.	6. Procesador de Texto
2. Estructura y componentes de una computadora.	7. Hoja electrónica de cálculo
3. Ambiente de trabajo.	8. Software educativo
4. Virus informático.	9. Programa de presentación
5. Redes de cómputo.	10. Trabajo final

Se observa que al finalizar la 5ª unidad llamada "Redes de cómputo", el alumno:

- Conocerá el desarrollo histórico de las redes
- Distinguirá los modos de acceso a la red
- Explicará las ventajas de trabajar en Red local
- Explicará el concepto de cliente-servidor
- Conocerá el concepto de Intranet e Internet
- Valorará la Información que recibe de Internet
- Describirá los servicios que ofrece la red

4.3 Educación Superior

Como se ha mencionado a lo largo de este trabajo de investigación, la seguridad informática se ha convertido en una necesidad para todos aquellos usuarios que tienen acceso a Internet, ya que desafortunadamente existen personas que buscan la manera de

obtener beneficios personales de manera ilícita por medio de las redes de comunicaciones. Razón por la que es necesario que los estudiantes en todos los niveles educativos reciban los conocimientos necesarios que les permitan resguardar correctamente sus bienes informáticos; así, se hace un análisis de los planes de estudio de las carreras de mayor demanda según datos emitidos por la Dirección General de Administración Escolar[40] que se imparten en las distintas facultades de la Universidad Nacional Autónoma de México, de manera que se logre apreciar si existen algunos temas relacionados con la seguridad informática. A continuación se muestra en la tabla 4.5 el plan de estudios correspondiente a la carrera de Arquitectura.

Tabla 4.5 Plan de estudios de la carrera de Arquitectura

Primer Semestre	**Segundo Semestre**
Introducción Histórico Crítica	Arquitectura en México. Siglo XX
Teoría de la Arquitectura I	Teoría de la Arquitectura II
Taller de Arquitectura I	Taller de Arquitectura II
Matemáticas Aplicadas	Matemáticas Aplicadas II
Sistemas Estructurales I	Sistemas Estructurales II
Tercer Semestre	**Cuarto Semestre**
Arquitectura, Ambiente y Ciudad I	Arquitectura, Ambiente y Ciudad II
Arquitectura Mesoamericana	Arquitectura en México. Siglos XVI al XVIII
Teoría de la Arquitectura III	Teoría de la Arquitectura IV
Taller de Arquitectura III	Taller de Arquitectura IV
Instalaciones I	Instalaciones II
Sistemas Estructurales III	Sistemas Estructurales IV
Extensión Universitaria I	Extensión Universitaria II
Quinto Semestre	**Sexto Semestre**
Diseño Urbano Ambiental	Taller de Arquitectura VI
Arquitectura en México. Siglo XIX	Instalaciones III
Teoría de la Arquitectura V	Sistemas Estructurales VI
Taller de Arquitectura V	Administración II
Sistemas Estructurales V	Extensión Universitaria IV
Administración I	Optativa
Extensión Universitaria III	
Séptimo Semestre	**Octavo Semestre**
Taller de Arquitectura VII	Taller de Arquitectura VIII
Administración III	Optativa
Optativa	Optativa
Optativa	Optativa
Optativa	Optativa
Noveno Semestre	**Decimo Semestre**
Seminario de Titulación I	Seminario de Titulación II

[40] https://www.escolar.unam.mx/folletodegose.pdf

Optativa	Práctica Profesional Supervisada
Optativa	
Optativa	
Optativa	

Como se observó, esta carrera no cuenta con asignaturas relacionadas a la computación, pero sí cuenta con un Centro de Cómputo el cual se encarga de implementar diversos programas de capacitación para los estudiantes y docentes, con el fin de desarrollar habilidades en el manejo de herramientas de software, creando sistemas de comunicación y de acceso a la información. A su vez cuenta con el laboratorio "Ángel Borja Navarrete", en el que se realiza el préstamo de equipo de cómputo, impresiones y se brindan asesorías a los estudiantes y al público en general.

En la Tabla 4.6 se muestra el plan de estudios de la carrera de Médico Cirujano, en el cual se aprecia que únicamente se imparten las asignaturas relacionadas con la carrera.

Tabla 4.6 Plan de estudios de la carrera Médico Cirujano

Primer Año	**Segundo Año**
Anatomía	Farmacología
Biología del Desarrollo	Fisiología
Bioquímica y Biología Molecular	Microbiología y Parasitología
Biología Celular y Tisular	Salud Pública II
Salud Pública I	Inmunología
Psicología Médica I	Cirugía I
Asignatura de libre elección	Asignatura de libre elección
Tercer Año	**Cuarto Año**
Propedéutica y Fisiopatología	Salud Pública IV
Patología	Historia y Filosofía de la Medicina
Medicina General I	Medicina General II
Psicología Médica II	Cirugía II
Salud Pública III	Asignaturas de libre elección
Genética Clínica	
Seminario Clínico	
Asignatura de libre elección	
Quinto Año	**Sexto Año**
Internado Médico	Servicio Social

En la tabla 4.7 se muestra el plan de estudios de la carrera de Derecho, en donde se observa que no se hace mención sobre alguna asignatura relacionada con la computación. De igual

forma, se sabe que existe un Centro de Cómputo llamado “Alfonso Quiroz Cuarón” en el cual se imparten cursos de computación como por ejemplo: Plataforma Windows y Procesador de palabras Word para Windows, Diseño de presentaciones Power Point y uso de herramientas de Internet. También se brindan los servicios de préstamo interno de equipo de cómputo, así como la consulta de internet, impresiones, correo electrónico y programas de Cómputo para invidentes.

Tabla 4.7 Plan de estudios de la carrera de Derecho

Primer Semestre	**Segundo Semestre**
Derecho Romano I	Derecho Romano II
Ética y Derechos Humanos	Metodología Jurídica
Historia del Derecho Mexicano	Teoría del Derecho
Introducción al Estudio del Derecho	Teoría de la Ley Penal y del Delito
Sociología General y Jurídica	Teoría de la Constitución
Teoría General del Estado	Bienes y Derechos Reales
Acto Jurídico y Personas	Teoría Económica
Tercer Semestre	**Cuarto Semestre**
Delitos en Particular	Derecho Procesal Civil
Derecho Constitucional	Derecho Administrativo I
Sistemas Jurídicos	Garantías Constitucionales
Teoría del Proceso	Contratos Civiles
Derecho Económico	Derecho Internacional Público
Obligaciones	Régimen Jurídico de Comercio Exterior
Sociedades Mercantiles	Títulos y Operaciones de Crédito
Quinto Semestre	**Sexto Semestre**
Derecho Administrativo II	Derecho Procesal Penal
Contratos Mercantiles	Derecho fiscal II
Derecho Fiscal I	Derecho Bancario y Bursátil
Derecho Internacional Privado	Derecho Internacional Privado II
Derecho Individual del Trabajo	Derecho Colectivo y Procesal del Trabajo
Familia y Sucesiones	Derecho Agrario
Amparo	Filosofía del Derecho
Séptimo Semestre	**Octavo Semestre**
Seguridad Social	Optativa de Preespecialidad
Optativa de libre elección o Primera Preespecialidad	Optativa de Preespecialidad
Optativa de libre elección o Primera Preespecialidad	Optativa de Preespecialidad
Optativa de libre elección o Primera Preespecialidad	Optativa de Preespecialidad

Optativa de libre elección o Primera Preespecialidad	Optativa de Preespecialidad
Optativa de libre elección o Primera Preespecialidad	Optativa de Preespecialidad

En la tabla 4.8 se muestra el Plan de Estudios de la carrera de Contaduría. Se observa que solo se imparten las asignaturas relacionadas a la carrera. Pero esta facultad cuenta con un centro de cómputo en el cual se imparten cursos a alumnos y al público en general sobre diversos temas como por ejemplo: office 2007, Web, lenguajes de programación, sistemas operativos, bases de datos, mantenimiento de equipos de cómputo y redes, entre otros.

Tabla 4.8 Plan de estudios de la Carrera de Contaduría

Primer Semestre	**Segundo Semestre**
Contabilidad I	Recursos Humanos
Matemáticas Financieras	Contabilidad II
Informática Básica	Estadística I
Administración Básica	Principios y Técnicas de Investigación
Macroeconomía	Derecho Mercantil
Teoría del Conocimiento	Finanzas I
Conceptos Jurídicos Fundamentales	Microeconomía
Tercer Semestre	**Cuarto Semestre**
Operaciones	Contabilidad IV
Contabilidad III	Sistemas de Control Interno
Finanzas II	Finanzas III
Costos I	Costos II
Derecho Laboral	Control de Gestión
Estadística II	Derecho Fiscal
Quinto Semestre	**Sexto Semestre**
Finanzas IV	Auditoría II
Contabilidad V	Régimen General de Empresas II: ISR e IAC
Presupuestos	Finanzas V
Régimen General de Empresas I: ISR e IAC	Auditoría Interna
Auditoría I	Contribuciones Indirectas y al Comercio Exterior
Séptimo Semestre	**Octavo Semestre**
Finanzas VI	Finanzas VII
Seguridad Social	
Personas Físicas no Empresarias	
Auditoría III	
Ética en las Organizaciones	

En la tabla 4.9 se muestra en plan de estudios de la carrera de Ciencias Políticas y Administración Pública:

Tabla 4.9 Plan de estudios de la carrera de Ciencias Políticas y Administración Pública

Primer Semestre	**Segundo Semestre**
Sociedad y Estado en México	Sociedad y Estado en México II
Historia Mundial I	Historia Mundial II
Introducción al Estudio del Derecho	Teoría General del Estado
Teoría de la Administración Pública I	Teoría de la Administración Pública II
Filosofía y Teoría Política I	Filosofía y Teoría Políticas II
Taller de Iniciación a la Investigación Social	Metodología Aplicada a las Ciencias Sociales
Tercer Semestre	**Cuarto Semestre**
Teoría Económica	Política Económica I
Geografía Económica y Política	Sistema Político Mexicano
Derecho Constitucional	Derecho Administrativo
Teoría de la Organización	Ciencia Política
Matemáticas	Estadística
Quinto Semestre	**Sexto Semestre**
Política Económica II	Gestión Económica del Estado Mexicano
Gobierno y Asuntos Públicos	Proceso de Gobierno en México
Desarrollo de Personal Público	Políticas Públicas I
Investigación de Operaciones	Gestión de Recursos Gubernamentales
Finanzas Públicas I	Finanzas Públicas II
Séptimo Semestre	**Octavo Semestre**
Proceso de Gobierno en México	Gobierno y Administración Urbana
Gerencia Pública	Proceso de Gobierno en México
Sistemas de Auditoría Gubernamental	Gerencia Social
Políticas Públicas II	
Noveno Semestre	
Laboratorio de Estudio de Casos	
Estadía Práctica	
Seminario de titulación	

Esta facultad cuenta con un laboratorio de cómputo en el cual se imparten cursos orientado a las asignaturas del sistema escolarizado, sistema abierto y Blended learning.

En la tabla 4.10 se muestra el plan de estudios correspondiente a la carrera de Economía, se aprecia que solo se imparten asignaturas correspondientes a la carrera. La Facultad cuenta con el CIFE (Centro de Informática de la Facultad de Economía) el cual se encarga de prestar el servicio informático y de red a las diferentes áreas académicas y administrativas. Este centro cuanta con la infraestructura de computadoras, servidores y red para prestar

servicios como: soporte técnico a computadoras y redes, préstamo de equipo de cómputo en salas, eventos; desarrollo de sistemas, correo electrónico, digitalización e impresión, entre otros.

Tabla 4.10 Plan de estudios de la carrera de Economía

Primer Semestre	**Segundo Semestre**
Historia Económica General I	Historia Económica General II
Economía Política I	Economía Política II
Introducción a la Teoría Económica	Teoría Microeconómica I
Taller de Economía Cuantitativa I	Taller de Economía Cuantitativa II
Introducción a los Métodos Cuantitativos	Matemáticas I
Contabilidad General y de Costos	Contabilidad Social
Investigación y Análisis Económica I	Investigación y Análisis Económica II
Tercer Semestre	**Cuarto Semestre**
Historia del Pensamiento Económico	Historia Económica de México I
Económica Política III	Economía Política IV
Teoría Microeconómica II	Teoría Macroeconómica
Taller de Economía Cuantitativa III	Taller de Economía Cuantitativa IV
Matemáticas II	Estadística
Análisis e Interpretación de Estados Financieros	Formulación y Evaluación de Proyectos
Investigación y Análisis Económico III	Investigación y Análisis Económico IV
Quinto Semestre	**Sexto Semestre**
Historia Económica de México II	Economía Mexicana I
Economía Política V	Estructura Económica Mundial Actual
Teoría Macroeconómica II	Economía Internacional
Taller de Economía Cuantitativa V	Taller de Economía Cuantitativa VI
Introducción a la Econometría	Teoría Monetaria y Política Financiera
Economía Industrial o Economía Agrícola	Finanzas Públicas
Investigación y Análisis Económico V	Desarrollo Económico
Séptimo Semestre	**Octavo Semestre**
Economía Mexicana II	Materia Clave III
Materia Clave I	Optativa Libre II
Materia Clave II	Optativa Libre III
Optativa Libre I	Optativa Tutorial I
Noveno Semestre	**Decimo Semestre**
Materia Clave IV	Optativa Libre V
Optativa Libre IV	Optativa Libre VI
Optativa Tutorial II	Optativa Tutorial IV
Optativa Tutorial III	

A continuación se muestra en la tabla 4.11 el plan de estudios correspondiente a la carrera de Química, se observa que solo se imparten las asignaturas relacionadas a ésta. La facultad cuenta con el Centro de Informática en el que se realizan los siguiente procesos: Administrar y dar soporte técnico a la red FQ, proporcionar soporte técnico a PC's, apoyar la administración de los servidores institucionales, apoyo estadístico a departamentos académicos, administración de la salas de cómputo para alumnos y asesoría en materia de cómputo.

Tabla 4.11 Plan de estudios de la carrera de Química

Primer Semestre	**Segundo Semestre**
Álgebra Superior	Cálculo II
Cálculo I	Estructura de la Materia
Ciencia y Sociedad	Física II
Física I	Laboratorio de Física
Química General I	Química General II
	Termodinámica
Tercer Semestre	**Cuarto Semestre**
Ecuaciones Diferenciales	Estadística
Equilibrio y Cinética	Fisicoquímica de Iónica y Electródica
Fundamentos de Espectroscopía	Química Analítica I
Química Inorgánica I	Química Cuántica I
Química Orgánica I	Química Inorgánica II
	Química Orgánica II
Quinto Semestre	**Sexto Semestre**
Fisicoquímica de Interfaces	Analítica Experimental I
Metrología	Cinética Química
Química Analítica	Química Analítica III
Química Inorgánica III	Química Inorgánica IV
Química Orgánica III	Química Orgánica IV
Optativa Sociohumanística	Optativa Sociohumanística
Séptimo Semestre	**Octavo Semestre**
Comunicación Científica	Analítica Experimental III
Química Analítica Instrumental I	Química Analítica Instrumental II
Analítica Experimental II	Seminario I
Bioquímica General	Trabajo de Investigación I
Laboratorio Unificado de Fisicoquímica	Optativa Disciplinaria Tipo B
Optativa Disciplinaria Tipo A	Optativa Disciplinaria Tipo B
Noveno Semestre	
Seminario II	
Trabajo de Investigación II	
Optativa Disciplinaria Tipo B	
Optativa Disciplinaria Tipo B	
Optativa Disciplinaria Tipo B	

En la tabla 4.12 se muestra en plan de estudios de la carrera de Trabajo social, en la cual se aprecia que únicamente se imparten las asignaturas correspondientes a la carrera, pero se cuenta con un laboratorio de cómputo y un Centro de Cómputo con acceso a internet. Así mismo se brinda apoyo a los usuarios y se dan asesorías en el uso de los equipos.

Tabla 4.12 Plan de estudios de la carrera Trabajo Social

Primer Semestre	**Segundo Semestre**
Teoría Social I	Teoría del Trabajo Social Comunitario
Teoría Económica I	Teoría Social II
Situación Internacional Contemporánea	Teoría Económica II
Análisis del Estado Mexicano	Situación Nacional Contemporánea
Necesidades y Problemas Sociales	Política Social
Lógica y Epistemología	Población y Medio Ambiente
	Investigación Social I
Tercer Semestre	**Cuarto Semestre**
Teoría de Grupos y Trabajo Social	Trabajo Social en la Atención Individualizada
Teoría Social III	Planeación y Desarrollo Social
Problemática Rural	Organización y Promoción Social
Estadística Aplicada a la Investigación Social I	Estadística Aplicada a la Investigación Social II
Movimiento y Participación Social	Práctica Comunitaria I
Programación Social	
Investigación Social II	
Quinto Semestre	**Sexto Semestre**
Desarrollo Regional	Familia y Vida Cotidiana
Salud Pública	Salud Mental
Problemática Urbana	Derechos Humanos
Evaluación de Proyectos Sociales	Educación Social
Práctica Comunitaria II	Práctica Regional I
Séptimo Semestre	**Octavo Semestre**
Bienestar Social	Situación Jurídica de la Familia
Procuración y Administración de Justicia	Psicología del Desarrollo Humano
Psicología Social	Comunicación Social
Administración Social	Práctica de Especialización I
Práctica Regional II	
Noveno Semestre	
Identidad y Cultura	
Análisis Institucional	
Práctica de Especialización II	

En la tabla 4.13 se muestra el plan de estudios de la carrera en Lengua y Literatura Hispánicas, al igual que las carreras anteriores, sólo se imparten las asignaturas correspondientes a ésta. También cuenta con un departamento de cómputo el cual se encarga de la administración, correcta distribución y aprovechamiento de los recursos informáticos de la facultad. Así mismo, cuenta sala multimedia, préstamo de equipo, servicio de impresión, soporte técnico, entre otros.

Tabla 4.13 Plan de estudios de la carrera en Lengua y Literatura Hispánicas

Primer Semestre	**Segundo Semestre**
Literatura Mexicana I	Literatura Mexicana II
Literatura Española I	Literatura Española II
Teoría de la Literatura I	Teoría de la Literatura II
Historia de la Cultura en España y América I	Historia de la Cultura en España y América II
Iniciación a la Investigación I	Iniciación a la Investigación II
Introducción a la lingüística I	Introducción a la lingüística II
Latín I	Latín II
Tercer Semestre	**Cuarto Semestre**
Literatura Mexicana III	Literatura Mexicana IV
Literatura Española III	Literatura Española IV
Teoría de la Literatura III	Teoría de la Literatura IV
Introducción a la Filosofía I	Introducción a la Filosofía II
Literatura Iberoamericana I	Literatura Iberoamericana II
Lexicología y Semántica I	Lexicología y Semántica II
Latín 3	Latín 4
Español 1	Español 2
Quinto Semestre	**Sexto Semestre**
Literatura Mexicana V	Literatura Mexicana VI
Literatura Española V	Literatura Española VI
Teoría de la Literatura V	Teoría de la Literatura VI
Fonética y Fonología I	Fonética y Fonología II
Literatura Iberoamericana III	Literatura Iberoamericana IV
Optativa	Optativa
Optativa	Optativa
Español 3	Español 4
Séptimo Semestre	**Octavo Semestre**
Literatura Mexicana VII	Literatura Mexicana VIII
Literatura Española VII	Literatura Mexicana XIX
Seminario de Investigación I	Seminario de Investigación II
Lingüística 1 Optativa de área	Lingüística 2 Optativa de área
Literatura Iberoamericana V	Optativa
Filología Hispánica I	Filología Hispánica II
Optativa	Optativa
Español 5	Optativa

En la tabla 4.14 se muestra el plan de estudios de la carrera de Medicina Veterinaria. Esta facultad cuenta con 6 laboratorios de cómputo distribuidos en los siguientes departamentos: Multimedia, Nutrición Animal y Bioquímica, Fisiología y Farmacología, Economía y Administración, Genética y Bioestadística y la Biblioteca "M.V. José de la Luz Gómez".

Tabla 4.14 Plan de estudios de la carrera de Medicina Veterinaria

Primer Semestre	**Segundo Semestre**
Biología Celular	Inmunología
Anatomía I	Fisiología
Histología y Biología del Desarrollo	Anatomía II
Introducción a la MVZ	Metodología de la Investigación
Tercer Semestre	**Cuarto Semestre**
Bacteriología y Micología	Patología General
Parasitología	Bioestadística
Virología	Legislación
Ecología	Etología
	Farmacología
Quinto Semestre	**Sexto Semestre**
Patología Sistémica	Patología Clínica
Nutrición	Alimentos y Alimentación
Mejoramiento Genético	Reproducción
Fundamentos de Cirugía	Epidemiología
	Imagenología
Séptimo Semestre	**Octavo Semestre**
Medicina y Zootecnia de Perros y Gatos	Producción Porcina
Medicina y Zootecnia de Equinos	Producción Avícola
Medicina y Zootecnia de Fauna Silvestre	Desarrollo Pecuario
Medicina Preventiva y Salud Pública	Admón. De Empresas Agropecuarias I
Manejo de Forrajes	
Noveno Semestre	**Decimo Semestre**
Producción Ovina	Producción Apícola
Producción Caprina	Producción Bovinos Leche
Animales de Laboratorio	Producción Acuícola
Admón. De Empresas Agropecuarias II	Producción Bovinos Carne
Aseg. De la Calidad de los Prod. y Subprod. Pecuarios	Producción Cunícola

En la tabla 4.15 se muestra el Plan de Estudios de la carrera de Cirujano Dentista, en el cual se aprecia que únicamente se imparten las asignaturas relacionadas a la carrera.

Tabla 4.15 Plan de estudios de la carrera de Cirujano Dentista

Primer Año	**Segundo Año**
Anatomía Dental	Fisiología
Anatomía Humana	Microbiología
Bioquímica	Odontología Preventiva y Salud Pública II
Educación para la Salud Bucal	Operatoria Dental
Histología, Embriología y Genética	Patología General e Inmunología
Materiales Dentales	Radiología
Odontología Preventiva y Salud Pública I	Técnicas Quirúrgicas
Oclusión	Emergencias Médico Dentales
	Propedéutica Médico Odontológica
	Anestesia
	Seminario de Historia de la Odontología
Tercer Año	**Cuarto Año**
Clínica Integrada de Endodoncia	Clínica de Prostodoncia
Clínica Integrada de Operatoria Dental	Clínica de Prótesis Dental Parcial Fija y Removible
Clínica Integrada de Periodoncia	Clínica Integrada
Exodoncia	Ortodoncia
Farmacología	Medicina Bucal
Patología Bucal	Cirugía Bucal
Prostodoncia Total	Odontopediatría
Prótesis Parcial Fija y Removible	
Quinto Año	
Clínica Integral Adultos	
Clínica Integral Niños	
Temas selectos	
Seminario de Nutrición	
Seminario de Oclusión	
Seminario de Administración	
Seminario de Deontología	

Se sabe que en esta facultad se cuenta con un centro de cómputo en el cual se brindan los servicios de préstamo de equipo para los estudiantes. De esta manera se observa que las Tecnologías de la Información están presentes en nuestra vida cotidiana y por ello es recomendable que se cree una conciencia sobre la importancia de la Seguridad Informática.

De manera particular se hace un análisis del plan de estudios de la carrera Ingeniería en Computación de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM). Este análisis consiste en la revisión general de las asignaturas relacionadas a la seguridad informática hasta llegar a la revisión particular de la elección del módulo de salida (Redes y Seguridad), que es al que se le prestará mayor atención.

En primera instancia se muestra el plan de estudios de la carrera de Ingeniería en Computación, el cual consta de 9 semestres y a partir del octavo semestre es donde se pueden elegir las asignaturas correspondientes al módulo de salida. Una vez que se ha escogido el módulo de salida, se procede a la elección de las asignaturas, las cuales se dividen en dos tipos; asignaturas obligatorias y optativas. En la tabla 4.16 se muestra el plan de estudios cuya actualización corresponde a la del año 2009.

Tabla 4.16 Plan de Estudios 2009 de la Facultad de Ingeniería de la UNAM

S	Asignaturas					
1	Algebra	Cálculo Diferencial	Geometría Analítica	Química y Estructura de Materiales (L+)		Cultura y Comunicación
2	Algebra Lineal	Cálculo Integral	Estática		Computación para Ingenieros (L+)	Introducción a la Economía
3	Ecuaciones Diferenciales	Cálculo Vectorial	Cinemática y Dinámica	Principios de Termodinámica y Electromagnetismo (L+)	Programación Avanzada y Métodos Numéricos	
4	Probabilidad y Estadística	Algoritmos y Estructuras de Datos	Estructura y Programación de Computadoras	Análisis de Sistemas y Señales	Literatura Hispanoamericana Contemporánea	Optativa de Ciencias Sociales y Humanidades
5	Ingeniería del Software	Estructuras Discretas	Sistemas Operativos	Circuitos Eléctricos (L+)	Diseño de Sistemas y Señales	
6	Lenguajes de Programación	Lenguajes Formales y Autómatas	Dispositivos y Circuitos Electrónicos	Sistemas de Comunicaciones (L+)	Microcomputadoras (L+)	Ética Profesional
7	Bases de Datos	Compiladores	Administración de Proyectos de Software	Redes de Datos (L+)	Arquitectura de Computadoras	Computación Gráfica
8	Sistemas de Control (L+)	Asignatura del Módulo Seleccionado	Asignatura del Módulo Seleccionado	Administración de Redes (L+)	Dispositivos de Almacenamiento y de E/S (L+)	Inteligencia Artificial
9	Asignatura del Módulo Seleccionado	Asignatura del Módulo Seleccionado	Asignatura del Módulo Seleccionado	Asignatura del Módulo Seleccionado u Optativa de Competencias Profesionales	Optativa de Competencias Profesionales	Recursos y Necesidades de México

Fuente: http://ingenieria.unam.mx/paginas/Carreras/planes2009/ingComputo_Plan.htm

4.1.3.1 Análisis general de las asignaturas relacionadas con la seguridad informática.

De la tabla anterior, se puede apreciar que a partir del segundo semestre, los alumnos cursan la asignatura; "Computación para Ingenieros", cuyo objetivo es el siguiente:
"El alumno conocerá la importancia de la computación e informática como herramienta para su desempeño académico y profesional de ingeniería. Empleará el software básico que le permita generar productos que resuelvan problemas matemáticos y de ingeniería".

Esta asignatura se imparte en el segundo semestre y pertenece al tronco común de todas las carreras de ingeniería, por lo que se vuelve importante que todo Ingeniero esté al tanto de las nuevas tendencias tecnológicas que se van generando día a día a nivel nacional e internacional, así cómo el aprendizaje sobre el diseño, desarrollo y manejo de software que le permita realizar aplicaciones para su propio beneficio sin importar la carrera que esté ejerciendo.

Es recomendable que todos los ingenieros generen conciencia sobre la importancia que van adquiriendo las Tecnologías de Información (TI), ya que son y seguirán siendo las herramientas de uso cotidiano, no sólo en los lugares de trabajo sino también en los hogares.

En el séptimo semestre los alumnos cursan la asignatura de *"Redes de Datos"* y posteriormente la de *"Administración de Redes"*, ambas incluyen un laboratorio. El objetivo de cada asignatura es el siguiente:

- **Redes de Datos:** *"El alumno comprenderá y aplicará los conocimientos de protocolos, métodos y estándares sobre redes de datos dentro de las siete capas del modelo ISO / OSI"*.
- **Administración de Redes:** *"El alumno conocerá, identificará y aplicará los diferentes enfoques, metodologías y técnicas que le permitan planear, organizar, integrar, dirigir y controlar redes de datos dentro del esquema de la Administración"*.

Es importante que todos los ingenieros en computación cursen estas asignaturas, independientemente del módulo de salida que elijan. Ello no implica que estén exentos de no utilizar equipos de cómputo y por ende que se esté libre de padecer algún tipo de ataque a los equipos de cómputo, al contrario, es conveniente que adquieran el conocimiento sobre el funcionamiento y todas sus implicaciones, como desde los tipos de red que existen hasta una buena planeación y control de ésta.

Es entonces que, a partir del octavo semestre el alumno elige el módulo de salida acorde a su perfil, pero como se ha mencionado anteriormente, de manera particular se hará hincapié al Módulo de Redes y Seguridad el cual corresponde directamente al tema de estudio "Seguridad Informática", el módulo contempla las siguientes asignaturas las cuales se muestran en la tabla 4.17.

Tabla 4.17 Módulo: Redes y Seguridad.

Obligatorias	Optativas
Criptografía	Desarrollo de software seguro
Seguridad Informática I	Análisis y diseño de redes de datos
Seguridad Informática II	Redes inalámbricas avanzadas
Arquitecturas Cliente / Servidor	Temas selectos de normalización
	Compresión de datos
	Codificación de audio y video
	Temas selectos de redes y seguridad
	Seminario de titulación
	Proyecto de investigación

De la tabla anterior, se puede apreciar que se deben cursar de manera obligatoria 4 asignaturas y únicamente se pueden elegir cómo máximo 2 de las 9 asignaturas optativas que ofrece la Facultad de Ingeniería. A continuación se analizan las asignaturas de carácter obligatorio.

4.1.3.2 Análisis de las asignaturas de carácter obligatorio en el módulo de salida de Redes y Seguridad

Para una adecuada formación académica en seguridad informática, los profesores de la Facultad de Ingeniería de la UNAM a través de varios análisis efectuados para llevar a cabo la actualización del plan de estudios correspondiente al año 2009, han determinado que las asignaturas a cursar de manera obligatoria sean las siguientes; C*riptografía, Seguridad Informática I, Seguridad Informática II y arquitecturas cliente/servidor*. Por lo tanto, se llevará a cabo un análisis general del contenido de cada asignatura con la finalidad de determinar qué tan adecuados son los temas acorde a los tiempos que se están viviendo y a su vez se que beneficie a los alumnos para que salgan mejor preparados de la Facultad de Ingeniería, tengan mejores oportunidades para su desarrollo profesional y cumplan con sus expectativas personales.

a) Criptografía

En primera instancia se analiza el objetivo de esta asignatura el cual dice:

"El alumno conocerá, explicará y aplicará los diferentes algoritmos criptográficos, metodologías y técnicas de cifrado que le permitan analizar, diseñar, desarrollar y/o seleccionar mecanismos y herramientas de seguridad de manera ética y profesional orientados a brindar seguridad informática, cuidando en todo momento que el trabajo realizado se enfoque al bienestar social".

La criptografía es una herramienta que se emplea para garantizar, en la medida de lo posible la integridad, confiabilidad y disponibilidad de la información que ha sido enviada de un equipo a otro por medio de una red de comunicaciones.

Por ello, se puede decir que esta asignatura es de suma importancia ya que le brinda al alumno la oportunidad de conocer y utilizar los diversos mecanismos de cifrado para implementar un buen sistema de seguridad, por ello es conveniente que se les apoye con material didáctico para que facilite su comprensión y sobre todo que ayude a mantenerse actualizados con las nuevas metodologías de cifrado que se van

desarrollando en el mundo y en nuestro país. Por ello la Facultad de Ingeniería ha publicado un libro titulado "Criptografía", el cual contiene desarrollado el temario de esta asignatura.

b) Seguridad Informática I

El objetivo de la asignatura es el siguiente:

"El alumno comprenderá y aplicará los métodos y elementos que le permitan planificar el desarrollo de una arquitectura de seguridad, con base en la identificación y análisis de amenazas, ataques y vulnerabilidades en los sistemas y redes de cómputo, enmarcados en una base ética".

Analizando el contenido de los temas, se puede apreciar que en esta asignatura se imparten los temas primordiales sobre la seguridad informática, como son: teoría, amenazas y vulnerabilidades, identificación de ataques y técnicas de intrusión, políticas de seguridad, análisis de riesgo y ética.

El aspecto a considerar que se tiene al impartir estos temas, es que su contenido será variable, es decir, derivado del avance tecnológico que se presenta día con día existirán nuevas formas de atacar a los sistemas y por consiguiente, nuevas metodologías, lo que obliga a mantenerse actualizados ante las nuevas tendencias.

c) Seguridad Informática II

El objetivo de esta asignatura es el siguiente:

"El alumno conocerá, identificará y aplicará los servicios y herramientas que le permitan implementar la seguridad informática dentro de una organización; conocerá, comprenderá y hará uso de las estrategias de monitoreo de los mecanismos de seguridad para administrar la seguridad dentro de una organización, a la vez podrá controlar los sucesos e incidentes de seguridad conociendo los aspectos sociales en el área de la seguridad informática".

Esta asignatura va seriada con lo antes mencionado (Seguridad Informática I), de tal manera que permita al alumno continuar adquiriendo los conocimientos sobre la seguridad informática y para ello se imparten los siguientes temas: implementación, monitoreo, administración, control, entorno social e impacto económico y nuevas tendencias y tecnologías.

El mundo de la seguridad informática es muy amplio y complejo porque abarca diversas metodologías acorde a lo que cada usuario requiera, es decir, no es lo mismo diseñar un sistema de seguridad para un usuario doméstico que para una organización, por ende son diferentes necesidades que demandan cada uno de estos, pero si bien es cierto, las bases teóricas siguen siendo las mismas, es decir, ambos requieren tener la seguridad de que la información que viaja a través de los sistemas de comunicación sea confiable, integra y sobre todo que se encuentre disponible en el momento que se desee.

Por ello la Facultad de Ingeniería ha desarrollado un libro de apuntes llamado "Fundamentos de Seguridad Informática" el cual fue editado en el año 2006. Cabe destacar que este material apoya a las dos asignaturas de Seguridad Informática y que éstas entraron en vigor en el nuevo plan de estudios correspondiente al año 2005 y las materias se comenzaron a impartir en el año 2006.

d) Arquitecturas Cliente/Servidor

El objetivo de esta asignatura es el siguiente:

"El alumno comprenderá y aplicará los conocimientos de protocolos, métodos y estándares sobre redes de datos, así como de criptografía y seguridad para que usando un lenguaje de programación cree programas bajo el esquema cliente/servidor"

Analizando el contenido de la asignatura, se aprecia que se contemplan temas como: Conceptos, creación de socket servidor y cliente; servidores y clientes sincronizados;

sockets broadcasting y multicasting; implantación de servidores con criptografía y código seguro; y creación de algoritmos de routing.

El ingeniero debe de conocer el funcionamiento básico de una arquitectura cliente/servidor, para su mejor entendimiento, ya que le permitirá adentrarse más a fondo al mundo de las redes de computadoras y a su vez comprenderá la manera en que se efectúan los ataques a los sistemas de información y así tener la capacidad de crear nuevas metodologías para evitar, en la medida de lo posible ser víctimas de ataques cibernéticos.

Es necesario entender dónde se encuentra almacenada la información y cómo es que viaja a través de las redes de datos para llegar a su destino. Considerando los avances tecnológicos que se viven día con día, hay que estar al pendiente de las nuevas tendencias que este tipo de arquitecturas pueda tener, ya que se ha observado que el punto es hacer más con menos, es decir, crear sistemas que sean más útiles, optimizando cierto tipo de recursos.

Además del bloque de asignaturas da carácter obligatorio, existe un grupo de asignaturas optativas que dependiendo del interés de cada estudiante podrán cursar alguna de ellas para enfatizar sus conocimientos, las materias que se ofertan son:

1. **Desarrollo de software seguro**
2. **Análisis y diseño de redes de datos**
3. **Redes inalámbricas avanzadas**
4. **Temas selectos de normalización**
5. **Compresión de datos**
6. **Codificación de audio y video**
7. **Temas selectos de redes y seguridad**
8. **Seminario de titulación**
9. **Proyecto de investigación**

Cada una de estas asignaturas permiten a los alumnos adquirir un mejor y mayor conocimiento acorde a sus intereses profesionales y así mismo especializarse en alguna rama de la seguridad informática e incluso aportar nuevas ideas para el beneficio de la sociedad y el propio mismo.

El objetivo de la Facultad de Ingeniería es que sus alumnos egresen con una preparación de calidad, por ello se vuelve indispensable mantener actualizados los planes de estudio y sobre todo, ofrecer un material de apoyo acorde a las necesidades existentes, como por ejemplo; libros, revistas, Internet, laboratorios, entre otros.

Capítulo 5
Propuesta

Las propuestas presentadas en este trabajo de investigación están basadas en los análisis realizados en los capítulos anteriores, por ello fue necesario conocer con mayor detalle la situación actual en materia de seguridad informática a la que se enfrentan la mayoría de los países a nivel mundial y en particular México, con la finalidad de visualizar cómo se encuentra nuestro país, hacia dónde se dirige y qué se requiere para cumplir las metas propuestas.

Si bien es cierto, la problemática principal a la que se enfrenta nuestro país, es a sus gobernantes, ya que no se invierte lo suficiente en cuanto a educación e investigación, a pesar de ello, se seguirá trabajando arduamente para impulsar una adecuada cultura en tecnologías de la información con la finalidad de aprovechar estos recursos al máximo, logrando así concientizar a los alumnos sobre la importancia de la seguridad informática e ir formando profesionistas altamente capacitados, quienes son los que dirigirán el rumbo de México.

Capítulo 5. Propuesta

5.1 Propuesta para los diferentes niveles educativos

Después de haber analizado de manera general la situación actual en la que se encuentra nuestro país en el nivel educativo básico:
Se propone que se sigan apoyando este tipo de proyectos, ya que ayudará a mejorar la calidad educativa generando en los alumnos enormes beneficios, como:

- Capacitación en el uso de la computadora, Internet, paquetería de oficina y otras aplicaciones didácticas para que estén mejor preparados.
- Apoyo a la economía familiar al reducir el gasto destinado a la renta de Internet.
- Disminuir los riesgos que implica el que un niño se traslade a un café Internet en un establecimiento público.
- Soporte a los equipos y al Internet vía la Mesa de Ayuda con la que cuenta el programa, lo cual garantizará que los equipos estén en buenas condiciones y el Internet esté disponible.

Por ello, se vuelve necesario aprovechar al máximo los recursos tecnológicos que se disponen hoy en día, para que los alumnos tengan una educación de calidad, ya que es fundamental para el desarrollo de nuestra sociedad y así ayudar a crear conciencia sobre una nueva cultura tecnológica que beneficiará a las futuras generaciones ayudándoles a enfrentar de la mejor manera posible los retos que nuestro país demanda.

Y en materia de seguridad se propone que se instrumenten cursos básicos de seguridad informática y de la información referentes a buenas prácticas y técnicas básicas de seguridad, a fin de que los niños aprendan a resguardar su información personal y hacerlo también con el uso de tecnologías de la información ya que actualmente el uso de las tecnologías para acceder a diversas aplicaciones, entre ellas las redes sociales, si bien son un beneficio social también pueden ser un foco de alerta en cuanto a seguridad se refiere.

Para darle continuidad a la educación que en materia de seguridad adquieran los jóvenes desde la infancia, *se propone* que al ingresar a la ENP, en el cuarto año en la asignatura

Informática se les den técnicas básicas de seguridad, uso de herramientas y buenas prácticas de seguridad.

De manera particular haciendo referencia al área 1 correspondiente a Ingeniería, que es cuando el alumno por segunda vez en el nivel medio superior tiene una asignatura relacionada con la seguridad informática llamada “Informática aplicada a la ciencia y la industria” la cual consta de 4 unidades:

1. Programación
2. Automatización de Procesos
3. La computadora y el Análisis Estadístico
4. Redes locales y Servicio de Red

Se analiza el contenido de la unidad 4 debido a su relación con la seguridad informática, el cual contempla los siguientes temas:

4.1 Tipos de Redes
4.2 Estándares de Redes
4.3 Hardware de Redes
4.4 Software de Redes
4.5 Canales de Comunicación
4.6 Servicios de Red

Así, *se propone* se incluya un tema sobre “**Seguridad Informática”** el cual contemple lo siguientes puntos:

4.7 Seguridad Informática
4.7.1 Definición de la Seguridad Informática
4.7.1.1 Principios
4.7.1.2 Confidencialidad
4.7.1.3 Disponibilidad

Se recomienda que se imparta de manera general, acorde a la madurez que se ha adquirido en este nivel educativo para que sea de fácil comprensión para los alumnos a fin de adentrarlos sobre la importancia de fomentar una nueva cultura en materia de seguridad informática.

Cabe mencionar que en nuestro país aún falta mucho por hacer, desafortunadamente el gobierno no invierte lo suficiente en educación, pero se debe hacer todo lo que esté al alcance para educar a las mujeres y a los hombres que mediante una formación integral, adquieran conocimientos sólidos y necesarios para cursar con éxito estudios superiores, con una mentalidad analítica, dinámica y crítica, la cual les permita ser conscientes de su realidad y comprometidos con la sociedad.

En cuanto al contenido del plan de estudios para alumnos del CCH, no se aprecian explícitamente objetivos de seguridad, por lo tanto *se propone* que en esta unidad se contemplen los siguientes objetivos.

El alumno:

- **Explicará el concepto de seguridad informática**
- **Conocerá las principales amenazas y vulnerabilidades**
- **Describirá las herramientas de seguridad existentes**

Otro aspecto importante es que en el quinto y sexto semestre (que es donde se imparten las materias de acuerdo al área que el alumno ha elegido), *se propone* que debería de tomarse

en cuenta la elección de una asignatura enfocada a la Seguridad Informática y que contemple los siguientes temas:

- Definición de la SI
  - Principios: Confidencialidad, Disponibilidad, Integridad
  - Importancia de la Seguridad Informática
  - Principales Amenazas y Vulnerabilidades
- Humanos
- Hardware
- Software
  - Políticas de Seguridad
  - Herramientas de Seguridad

Así mismo como se ha planteado para la ENP, *se propone* algo muy similar para el CCH, cuyo objetivo es que los alumnos adquieran los conocimientos básicos sobre la seguridad informática y vayan generando conciencia sobre ésta, brindándole dos oportunidades, la primera es que todo alumno que ingrese a la educación media superior, tenga la oportunidad de conocer lo básico sobre seguridad informática y en segundo lugar es que los alumnos que elijan el área de computación tengan un mejor dominio del tema y así tener la oportunidad de ingresar a la educación superior con una preparación más eficaz y eficiente.
Se sabe que la tecnología avanza día con día, lo que obliga a mantenerse actualizados con las nuevas tendencias tecnológicas, creando hábitos que permitan formar profesionistas altamente capacitados y que éstos sean quienes lleven esta disciplina a los lugares de trabajo, logrando así impactar en la economía y productividad de nuestro país.

Es importante que a los alumnos de los CCH y ENP se les haga mención sobre la seguridad informática a fin de que conozcan un panorama general de lo importante que se vuelve el hecho de tener hábitos adecuados para garantizar en la medida de lo posible, que establezcan una conexión confiable y segura, teniendo en cuenta los conocimientos vistos en clase y llevarlos a la práctica para evitar que sean víctimas de ataques cibernéticos debido al desconocimiento que tienen los jóvenes sobre la seguridad informática.

Capítulo 5. Propuesta

Con base en el análisis realizado a nivel licenciatura se hace necesario que se preparen a las futuras generaciones, brindándoles los conocimientos adecuados en materia de seguridad informática conforme a los tiempos que se están viviendo, de tal manera que adquieran la capacidad de resolver problemas e incluso aporten nuevas ideas para combatir de la mejor manera posible los ataques a los que están expuestos las redes de computadoras día con día.

Así, a nivel superior, *se propone* que en todas las facultades se instaure un programa de apoyo en las áreas de cómputo destinado a brindar orientación y capacitación a los estudiantes a fin de mantener segura su información, de esta manera se logrará crear una cultura en seguridad informática que beneficiará a los estudiantes de las diferentes carreras que imparte la UNAM.

Por lo tanto, para darle continuidad a la educación sobre la seguridad informática y una vez que se analizaron de manera general las asignaturas que se imparten en la Facultad de Ingeniería de la Universidad Nacional Autónoma de México las cuales son de carácter obligatorio correspondiente al módulo de salida de Redes y Seguridad, *se propone* que se lleve a cabo la actualización del libro “Fundamentos de Seguridad Informática”, acorde al año en curso, para satisfacer las necesidades presentes y futuras, ya que en todo este tiempo ha habido avances que requieren que se les brinde una atención adecuada, de tal manera que se sigan cubriendo las expectativas de aprendizaje que el plan de estudios requiere.

Este libro fue editado en el año 2006, su objetivo es proporcionar los temas fundamentales sobre seguridad informática, el cual se relaciona particularmente con las asignaturas de Seguridad Informática I y II.
Este tipo de asignaturas promueve que tanto los profesores como los alumnos se mantengan actualizados ante las nuevas tendencias que van surgiendo ya que en esta época es cuando más se requiere de profesionistas con conocimientos sólidos y bases éticas firmes que beneficien a la sociedad y que aporten nuevas propuestas para crear una nueva cultura en tecnologías de información aprovechando así el uso eficiente del Internet. Por lo que se vuelve indispensable que los futuros ingenieros adquieran los conocimientos necesarios para enfrentar de la mejor manera posible los retos que el país demanda.

5.2 Modelo educativo

Después de haber realizado el estudio correspondiente a la educación en materia de seguridad en nuestro país, se presenta a manera de resumen en la figura 5.1 el estado de la educación en México y en líneas punteadas se muestran las actividades que *se proponen* para complementar la educación de los connacionales desde la educación básica hasta el nivel licenciatura, donde se exhorta a dar continuidad a lo planteado por el Gobierno del DF y de esa manera los alumnos adquieran los conocimientos sobre seguridad informática acorde al nivel educativo en el que se encuentren.

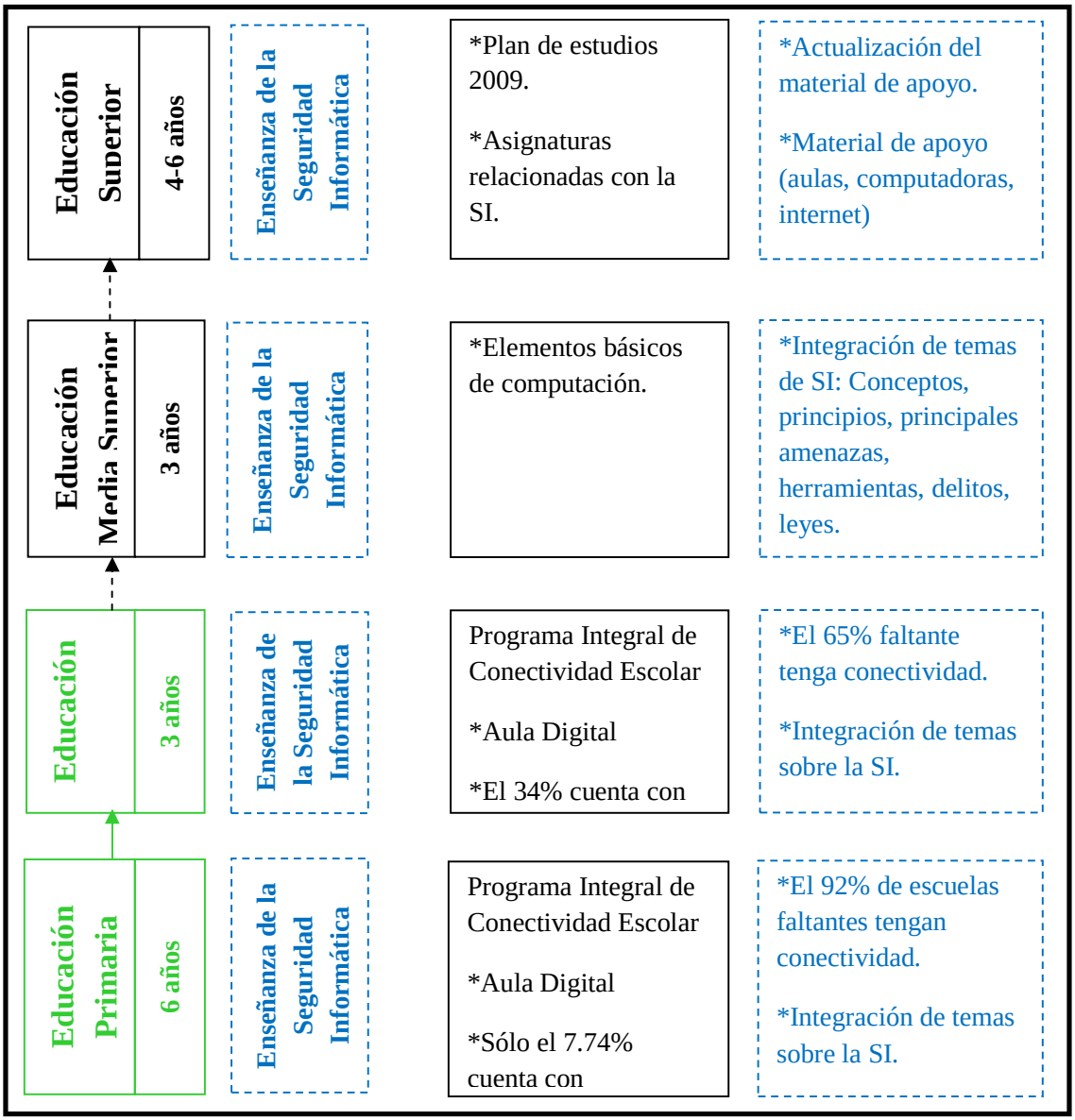


Figura 5.1 Cuadro resumen de la educación en México

Cabe destacar que para lograr la enseñanza sobre la seguridad informática es necesario contar con un modelo educativo que permita la realización de dicho objetivo. Por lo tanto, para el caso particular de este trabajo de investigación, me parece importante definir que es un modelo educativo, el cual se muestra a continuación:

- *"Es una recopilación o síntesis de distintas teorías y enfoques pedagógicos que orientan a los docentes en la elaboración de los programas de estudios y en la sistematización de los procesos de enseñanza y aprendizaje. Un modelo educativo es un patrón conceptual en el cual se esquematizan las partes y elementos de un programa de estudios".*[43]

Por lo tanto, el docente aprende a elaborar, operar un plan de estudios y a sistematizar los procesos de enseñanza y aprendizaje. Por ello se propone un modelo educativo en materia de Seguridad Informática que ayude a los alumnos desde la educación básica hasta el nivel superior a adquirir los conocimientos básicos sobre ésta.

Por ello, es importante que los alumnos tengan los conocimientos necesarios sobre las principales amenazas que existen en nuestro país, así como de las herramientas que existen, para evitar en la medida de lo posible ser víctimas de cualquier tipo de amenaza y aprender a prevenirlas y si fuese necesario a mitigarlas.

De esta manera se creará conciencia en los alumnos sobre la seguridad de la información y lo llevarán a la práctica en su vida cotidiana de manera segura y eficiente, reflejando resultados positivos en el desarrollo de nuestro país, ya que son ellos quienes tendrán la responsabilidad de convertir a México en un país competitivo y con un mejor nivel educativo.

[22] http://definicion.de/modelo-educativo/

A continuación en la figura 5.2 se muestra el Modelo educativo propuesto sobre Seguridad Informática.

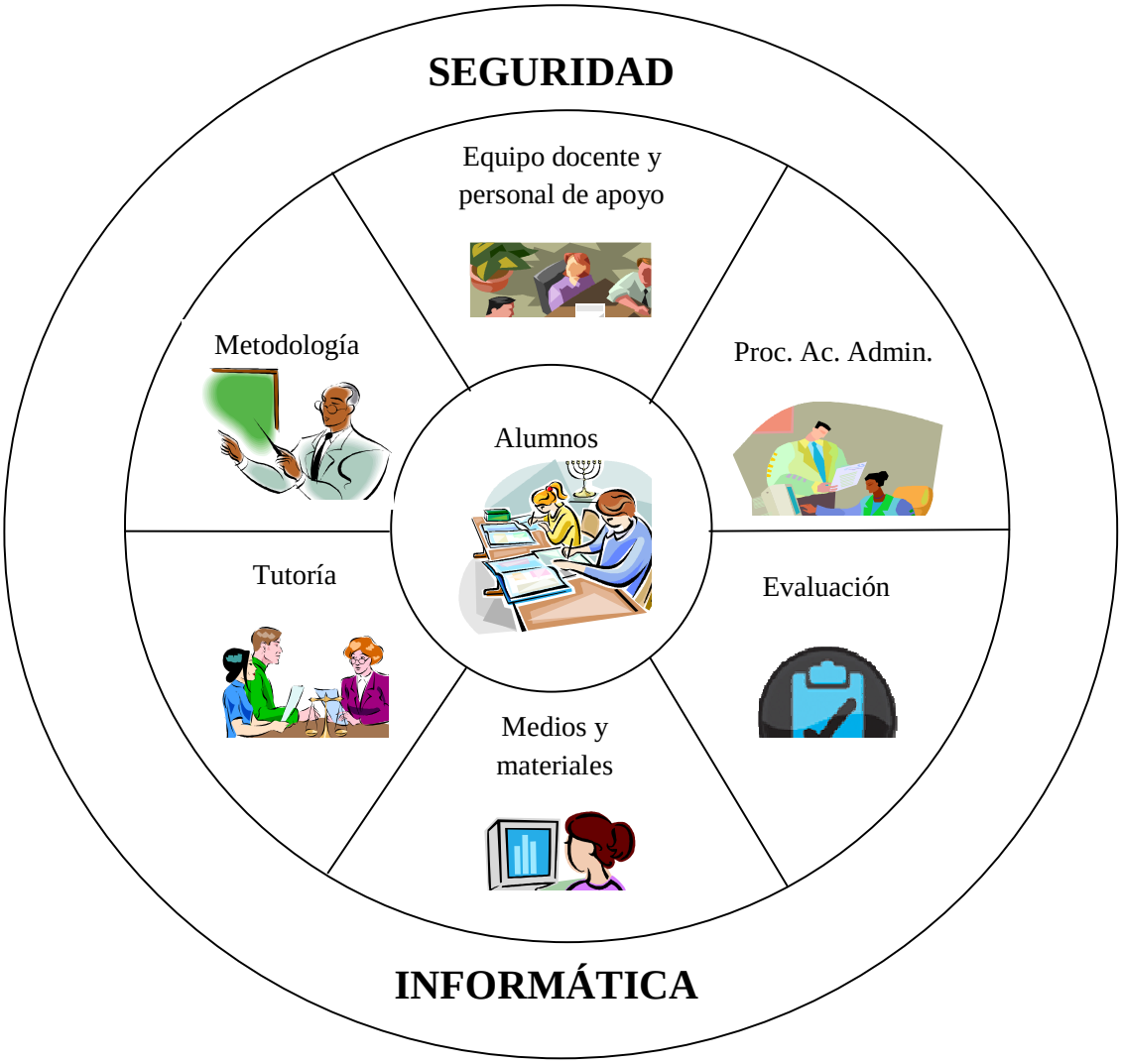


Figura 5.2 Modelo educativo de seguridad informática

Como se aprecia de la figura 5.2, para que existan buenas prácticas en materia de seguridad informática, es necesario que los alumnos cuenten con 6 aspectos diferentes los cuales se describen a continuación:

Alumnos: Son los niños, adolescentes y jóvenes a quienes va dirigido la enseñanza de la seguridad informática, puesto que ellos llevarán a la práctica lo aprendido a lo largo de su trayectoria como estudiantes.

Equipo docente y personal de apoyo: Está conformado por profesores que ya fueron capacitados en materia de seguridad informática y académicos que cuenten con una experiencia profesional sólida y docente.

Metodología: Es el conjunto de actividades y recursos que se seleccionan para desarrollar un proceso de aprendizaje. Para el caso particular de este modelo propuesto, se refiere a una enseñanza presencial, es decir, maestro – alumno ya que incita la participación entre los estudiantes, para su mejor desarrollo de aprendizaje.

Tutorías: El tutor constituye el enlace fundamental entre el participante y la Universidad. Cada tutor es responsable de la conducción de un grupo de alumnos, acompañándolos a lo largo de sus procesos de estudio y aprendizaje. También orienta a los alumnos en la búsqueda de información y lo asesora en su desarrollo académico.

Medios y Materiales: Se refiere a los medios de comunicación y material de desarrollo para el aprendizaje de la seguridad informática. Estos pueden ser, apuntes, tareas, libros, revistas, internet, correo electrónico, foros de discusión, entre otros.

Evaluación: Los alumnos son evaluados para conocer el nivel de aprendizaje que han adquirido a lo largo del curso, de esa manera se detectan las posibles fallas que puedan existir o en caso contrario, la aceptación que adquirieron a lo largo del curso.

Procesos académico administrativos: Se refiere a la oficina en donde se analizan los proyectos planteados, así como el presupuesto para invertir en seguridad informática. También se lleva a cabo la realización de trámites, pagos, certificaciones, entre otros.

Las ventajas de este tipo de modelo educativo son:

- El alumno es responsable de su propio proceso de aprendizaje.
- La interacción con el docente, tutores y demás alumnos.
- El tutor se encargara de informarle al alumno sobre su desempeño a lo largo del proceso de aprendizaje.
- El alumno será capaz de manejar las herramientas básicas de la computación de manera eficiente y segura.
- Será capaz de crear conciencia sobre la importancia de la seguridad informática y lo llevará a la práctica en su vida cotidiana.

Después de haber planteado la propuesta, se espera que se aplique a todos los niveles educativos no importando la profesión que tengan los alumnos ya que actualmente la computadora se ha convertido en una herramienta de trabajo de uso cotidiano que requiere se le preste la atención adecuada para su buen manejo.

Si se cuentan con los conocimientos sobre seguridad informática desde la educación básica, es muy probable que los futuros profesionistas tengan las habilidades para enfrentar la problemática que se vive hoy en día y la única manera de lograr que las empresas adquieran mayor compromiso con la seguridad informática, es invirtiendo también en educación.

Capítulo 6
Contenidos desarrollados

Los temas que se desarrollan en este capítulo se basan en la realización de un análisis exhaustivo de los programas de estudio correspondientes a las asignaturas de Seguridad Informática I y II, dando como resultado la actualización del material de apoyo que se brinda a los alumnos de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México.

Es necesario destacar que el mundo de la seguridad informática es muy amplio y complejo, por ello se contemplaron incluir estos temas ya que beneficiará al buen aprendizaje de ambas asignaturas, logrando así cumplir con los objetivos de cada una de éstas.

Los temas propuestos para actualizar el material de apoyo se ven reflejados a continuación, de manera que se muestra el índice modificado del libro ya mencionado (Fundamentos de Seguridad Informática) destacando con letra cursiva y en negritas los temas que se le han agregado a éste.

"Fundamentos de Seguridad Informática"
CONTENIDO

CAPÍTULO 1
CONTEXTO DE LA SEGURIDAD
1.1 Panorama general
1.2 Metodología
1.3 Perfiles de protección
    1.3.1 Estructura de los perfiles de protección
    1.3.2 Administración de la seguridad

CAPÍTULO 2
NORMATIVIDAD
2.1 Definiciones
2.2 Niveles de seguridad
    2.2.1 Criterios comunes
    2.2.2 Estándar ISO 17799
    2.2.3 Familia de Normas ISO/IEC 27000
    2.2.4 Identificación de los factores de riesgo
    2.2.5 Metodologías para el análisis de riesgos

CAPÍTULO 3
AMENAZAS Y VULNERABILIDADES
3.1 Clasificación general de amenazas
    3.1.1 De humanos
    3.1.2 Errores de hardware
    3.1.3 Errores de la red
    3.1.4 Problemas de tipo lógico
    3.1.5 Desastres
3.2 Clasificación general de vulnerabilidades
3.3 Clasificación general de amenazas o ataques inherentes a las redes
    3.3.1 Ataques pasivos
    3.3.2 Ataques activos
3.4 Métodos de ataque
    3.4.1 Preparación y planteamiento
    3.4.2 Activación
    3.4.3 Ejecución
    3.4.4 Ataques en escudos

CAPÍTULO 4
SERVICIOS DE SEGURIDAD
4.1 Definición
4.2 Clasificación
- 4.2.1 Confidencialidad
- 4.2.2 Autenticación
- 4.2.3 Integridad
- 4.2.4 No repudio
- 4.2.5 Control de acceso
- 4.2.6 Disponibilidad

CAPÍTULO 5
POLÍTICAS DE SEGURIDAD
5.1 Misión de la organización (sus objetivos)
5.2 Definición de política
- 5.2.1 Principios fundamentales

5.3 Definición de modelos
- 5.3.1 Criterios
- 5.3.2 Modelos de control de acceso
- 5.3.3 Modelos de flujo de información
- 5.3.4 Modelos de integridad

5.4 Identificación y establecimiento de políticas de seguridad

CAPÍTULO 6
ANALISIS DEL RIESGO
6.1 Definiciones
6.2 Tipos de análisis del riesgo
- 6.2.1 Análisis cuantitativo del riesgo
- 6.2.2 Análisis cualitativo del riesgo

6.3 Cómo establecer los requerimientos y riesgos de seguridad
6.4 Pasos del análisis del riesgo
6.5 Consideraciones adicionales durante el análisis del riesgo

CAPÍTULO 7
HERRAMIENTAS DE SEGURIDA
7.1 Introducción
7.2 Principales Herramientas
- ***7.2.1 Monitoreo***
- ***7.2.2 Auditoría***
- ***7.2.3 Criptografía***
- ***7.2.4 Escaneo***
- ***7.2.5 Filtrado***
- ***7.2.6 Detección de Intrusos***
  - ***7.2.1 Tipos de Intrusos***
  - ***7.2.2 Composición de los IDS***

7.2.3 Clasificación de los IDS
7.3 Autenticación

CAPÍTULO 8
AUDITORIA
8.1 Definición
8.2 Auditoría interna y auditoría externa
8.3 Características de la Auditoría informática
8.4 Tipos y clases de auditorías
8.5 Fases de una auditoría
8.6 Auditoría de la seguridad de la información
8.7 Enfoques de la Auditoría Informática
8.8 Herramientas y técnicas para la auditoría informática
8.9 Perfil Profesional del auditor informático

CAPITULO 9
SEGURIDAD EN REDES INALAMBRICAS
9.1 Definición de la seguridad inalámbrica
9.2 Implementación de los atributos de seguridad
9.3 Servicios de seguridad en redes inalámbricas
9.3.1 Confidencialidad
9.3.2 Autenticación
9.3.3 Integridad de datos en redes inalámbricas
9.3.4 Disponibilidad en redes inalámbricas
9.3.5 No repudio (rendición de cuentas)
9.4 Principales amenazas de seguridad en las redes inalámbricas

CAPÍTULO 10
SEGURIDAD EN BASES DE DATOS
10.1 Introducción
10.2 Confidencialidad de la BD
10.2.1 Deducción de información confidencial de una BD
10.3 Disponibilidad de la BD
10.4 Integridad de la BD
10.5 Mecanismo de seguridad en SGBD

*CAPITULO **11***
ÉTICA INFORMÁTICA
11.1 Concepto de ética
11.2 Código deontológico
11.3 Ética profesional
11.3.1 Código de ética profesional del ingeniero mexicano
11.3.2 Código de ética y ejercicio profesional de la ingeniería de software del Institute of Electrical and Electronics Engineer (IEEE)
11.3.3 Código de ética universitario a la comunidad universitaria
11.4 La formación ética

11.5 Contenidos de la ética informática
11.6 Código deontológico
11.7 Objetivos del código deontológico
11.8 Funciones del código deontológico
11.9 Código deontológico de los ingenieros informáticos

*CAPITULO **12***
LEGISLACIÓN Y DELITOS INFORMÁTICOS
12.1 Panorama mundial
    12.1.1 Antecedentes externos
    12.1.2 Ley modelo sobre comercio electrónico
    12.1.3 Comisión de las Naciones Unidas para la ley del comercio internacional
12.2 Contexto nacional
    12.2.1 Reorientación de la política informática
    12.2.2 Normatividad en informática
    12.2.3 Foros de consulta
12.3 Delitos informáticos
12.4 Tipos de delitos informáticos
12.5 Legislación Internacional

GLOSARIO
BIBLIOGRAFÍA

Es imprescindible que los futuros ingenieros conozcan las diferentes metodologías que existen para el análisis de riesgos y así mismo los estándares de la Familia ISO/IEC 27000, ya que les permitirá adquirir una visión más amplia sobre lo importante que se vuelve, principalmente para las organizaciones el hecho de tener como base estos estándares, los cuales se desarrollan a continuación:

6.1 Familia de Normas ISO / IEC 27000

Desde 1901 y como primera entidad de normalización a nivel mundial, BSI (British Standars Institution) es responsable de la publicación de importantes normas como:

- 1979 Publicación BS 5750 – ahora ISO 9001
- 1992 Publicación BS 7750 – ahora ISO 14001
- 1996 Publicación BS 8800 – ahora OHSAS (Occupational Healt and Safety Assessment Series) 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa (británica o no) un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7788-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO sin cambios sustanciales como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión, de manera que para el año 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de

Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información. En la Figura 6.1 se puede observar de manera resumida lo antes mencionado.

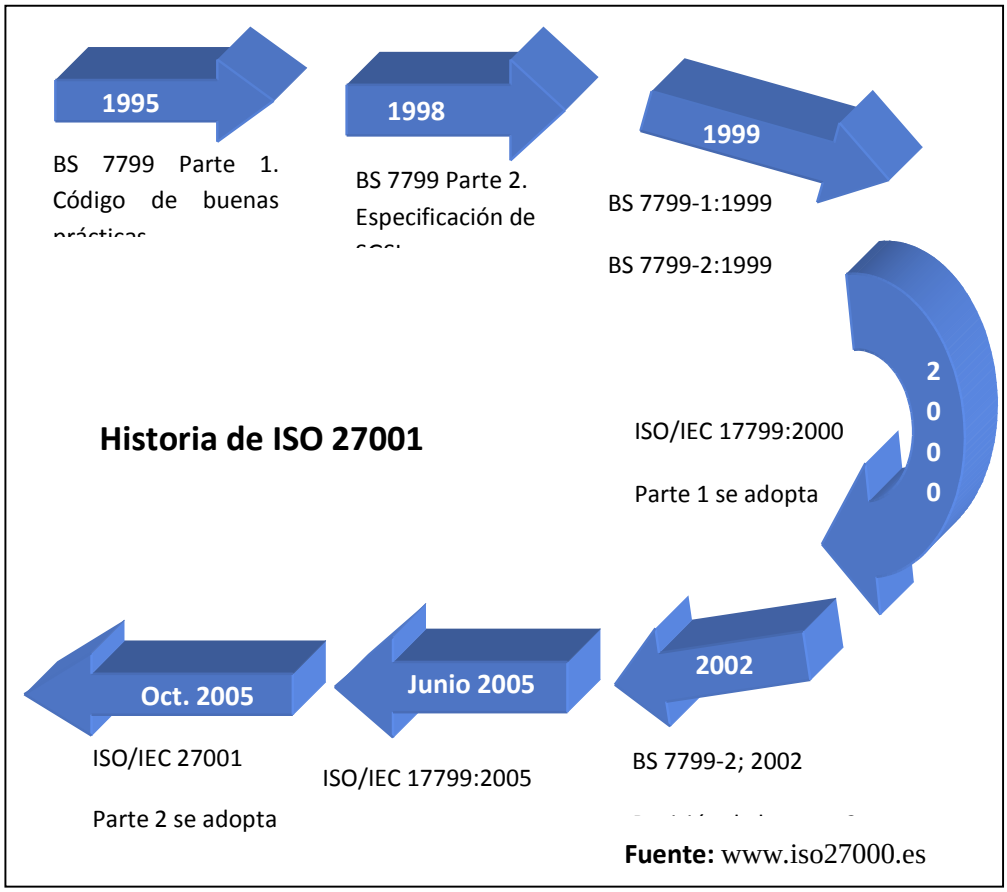


Figura 6.1 Historia de ISO 27001

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), esta serie contiene las mejores prácticas recomendadas para la Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI), hasta principios de febrero de 2011 la mayoría de estas normas se encuentran en preparación e incluyen:

a) **ISO/IEC 27000:** Publicada el 1 de Mayo de 2009. Esta norma proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción del proceso Plan-Do-Check-Act y términos y definiciones que se emplean en toda la serie 27000[45].

b) **ISO/IEC 27001:** Publicada el 15 de octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

c) **ISO/IEC 27002**: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

d) **ISO/IEC 27003:** Publicada el 1 de Febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

e) **ISO/IEC 27004:** Publicada el 7 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para

[45] http://www.iso27000.es/iso27000.html

determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

f) **ISO/IEC 27005**: Publicada el 4 de Junio de 2008. No certificable. Proporciona las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

g) **ISO/IEC 27006**: Publicada el 1 de Marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

h) **ISO/IEC 27007**: En fase de desarrollo, consistirá en una guía de auditoria de un SGSI, como complemento a lo especificado en ISO 19011.

i) **ISO/IEC 27008**: En fase de desarrollo. Consistirá en una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

j) **ISO/IEC 27010:** En fase de desarrollo. Es una norma en 2 partes, que consistirá en una guía para la gestión de la seguridad de la información en comunicaciones inter-sectoriales.

k) **ISO/IEC 27011**: Publicada el 15 de Diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-TX.1051. ITU (Unión Internacional de Telecomunicaciones).

l) **ISO/IEC 27012:** En fase de desarrollo. Consistirá en un conjunto de requisitos (complementarios a ISO/IEC 27001) y directrices (complementarias a ISO/IEC

27002) de gestión de seguridad de la información en organizaciones que proporcionen servicios de e-Administración.

m) ISO/IEC 27013: En fase de desarrollo. Consistirá en una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

n) ISO/IEC 27014: En fase de desarrollo. Consistirá en una guía de gobierno corporativo de la seguridad de la información.

o) ISO/IEC 27015: En fase de desarrollo. Consistirá en una guía de continuidad de SGSI para organizaciones del sector financiero y de seguros.

p) ISO/IEC 27031: En fase de desarrollo, consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

q) ISO/IEC 27032: En fase de desarrollo, consistirá en una guía relativa a la ciberseguridad.

r) ISO/IEC 27033: Norma dedicada a la seguridad de redes, consiste en 7 partes: 27033-1, conceptos generales; 27033-2, directrices de diseño e implementación de seguridad en redes; 27033-3, escenarios de redes de referencia; 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad; 27033-5, aseguramiento de comunicaciones mediante VPNs; 27033-6, convergencia IP; 27033-7, redes inalámbricas.

s) ISO/IEC 27034: En fase de desarrollo, consistirá en una guía de seguridad en aplicaciones informáticas.

t) ISO/IEC 27035: En fase de desarrollo, consistirá en una guía de gestión de incidentes de seguridad informática.

u) ISO/IEC 27036: En fase de desarrollo, consistirá en una guía de seguridad en outsourcing (externalización de servicios).

v) ISO/IEC 27037: En fase de desarrollo, consistirá en una guía de identificación, recopilación y preservación de las evidencias digitales.

w) ISO/IEC 27799: Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO/IEC 27002 y es un complemento de esa norma. ISO 27799:2008

especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, videos e imágenes médicas), sea cual fuere el medio utilizado para almacenar(de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para el transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida.

Beneficios de la familia de normas 27000

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través de medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, entre otros).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

6.2 Metodologías para el análisis de riesgo

En el mundo de la seguridad informática no sólo se disponen de normas de análisis de riesgos, también existen metodologías ampliamente conocidas y de uso generalizado. Las Principales son MAGERIT, EBIOS, CRAMM y OCTAVE, las cuales se detallan a continuación:

MAGERIT: Es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas". Es una metodología de carácter público, perteneciente al Ministerio de Administraciones Públicas y fue elaborado por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales (SSITAD), del Consejo Superior de Informática.

Se trata de una metodología para conocer el riesgo al que está sometida una información y qué tan segura (o insegura) está.

Objetivos de MAGERIT:

- **Estudiar los riesgos** que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un **análisis de los riesgos** que implica la evaluación del *impacto* que una violación de la seguridad tiene en la organización; señala los *riesgos* existentes, identificando las *amenazas* que acechan al sistema de información y determina la *vulnerabilidad* del sistema de prevención de dichas amenazas, obteniendo unos resultados.

- Los resultados del análisis de riesgos permiten a la ***gestión de riesgos*** **recomendar las medidas** apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.
- Como **objetivo a más largo plazo,** MAGERIT prepara su lógica articulación con los mecanismos de evaluación, homologación y certificación de seguridad de sistemas de información (ITSEC, Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistemas de Información).

La Aplicación de MAGERIT permite:

- *Aportar racionalidad en el conocimiento del estado de seguridad* de los Sistemas de Información y en la introducción de medidas de seguridad.
- *Ayudar a garantizar una adecuada cobertura en extensión*, de forma que no haya elementos del sistema de información que queden fuera del análisis, y *en intensidad*, de forma que se alcance la profundidad necesaria en el análisis del sistema.
- *La incrustación de mecanismos de seguridad en el corazón mismo de los sistemas de información:*
  a) Para paliar las insuficiencias de los sistemas vigentes.
  b) Para asegurar el desarrollo de cualquier tipo de sistemas, reformados o nuevos, en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y mantenimiento.

El análisis y Gestión de Riesgos es el “corazón” de toda actuación organizada en materia de seguridad y de la gestión global de la seguridad. Influye en las Fases y actividades de tipo estratégico (implicación de la dirección, objetivos, políticas) y condiciona la oportunidad de las fases y actividades de tipo logístico (planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento). Así cómo se muestra en la figura 6.2.

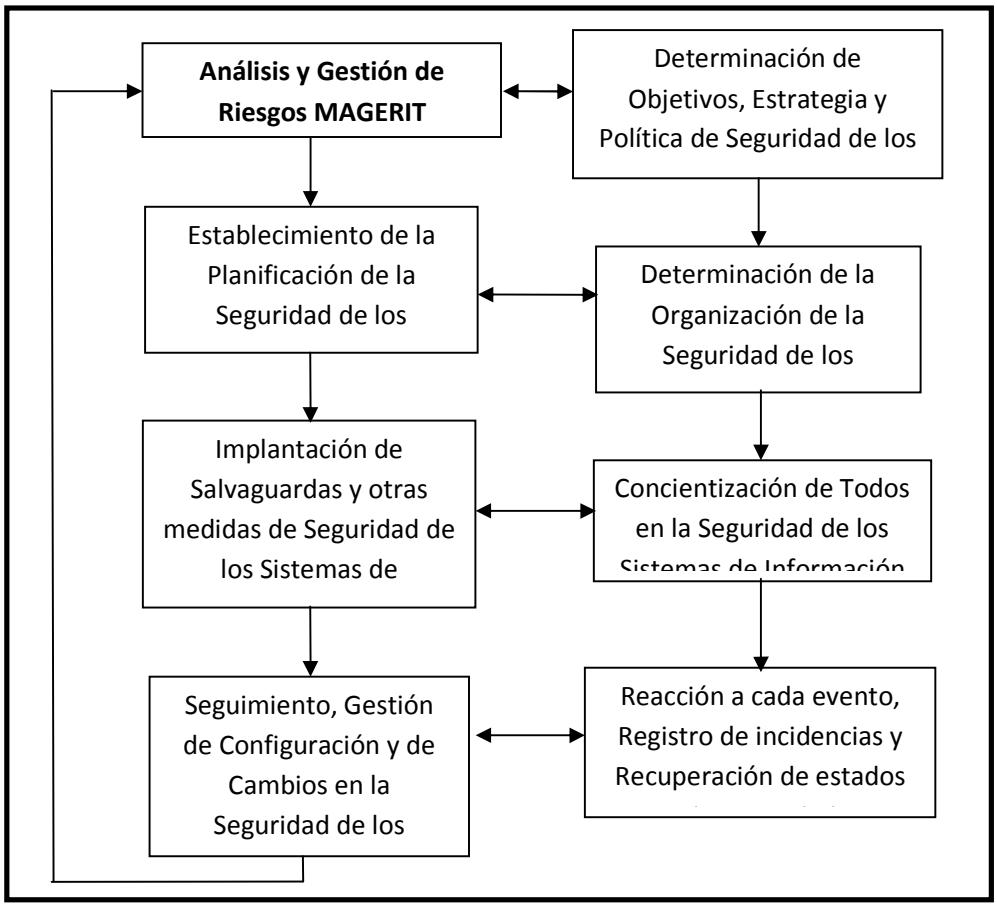


Figura 6.2 Análisis y Gestión de Riesgos de MAGERIT

Tipos de proyectos

MAGERIT responde a las necesidades de un amplio espectro de intereses de usuarios con un enfoque amplio de adaptación a cada organización y a sensibilidades diferentes en Seguridad de los Sistemas de Información. Las diferencias residen en tres cuestiones fundamentales:

- **Situación:** dentro del "ciclo de estudio"; marco estratégico, planes globales, análisis de grupos de múltiples activos, gestión de riesgos de activos concretos, determinación de mecanismos específicos de salvaguarda.
- **Envergadura:** complejidad e incertidumbre relativas del dominio estudiado, tipo de estudio más adecuado a la situación (corto, simplificado, entre otros), granularidad adoptada.

- **Problemas específicos que se deseen solventar:** Seguridad lógica, Seguridad de Redes y Comunicaciones, Planes de Emergencia y Contingencia, Estudios técnicos para homologación de sistemas o productos, Auditorías de seguridad.

Estructura de MAGERIT: El modelo normativo de MAGERIT se apoya en tres submodelos (así como se muestra en la figura 6.3):

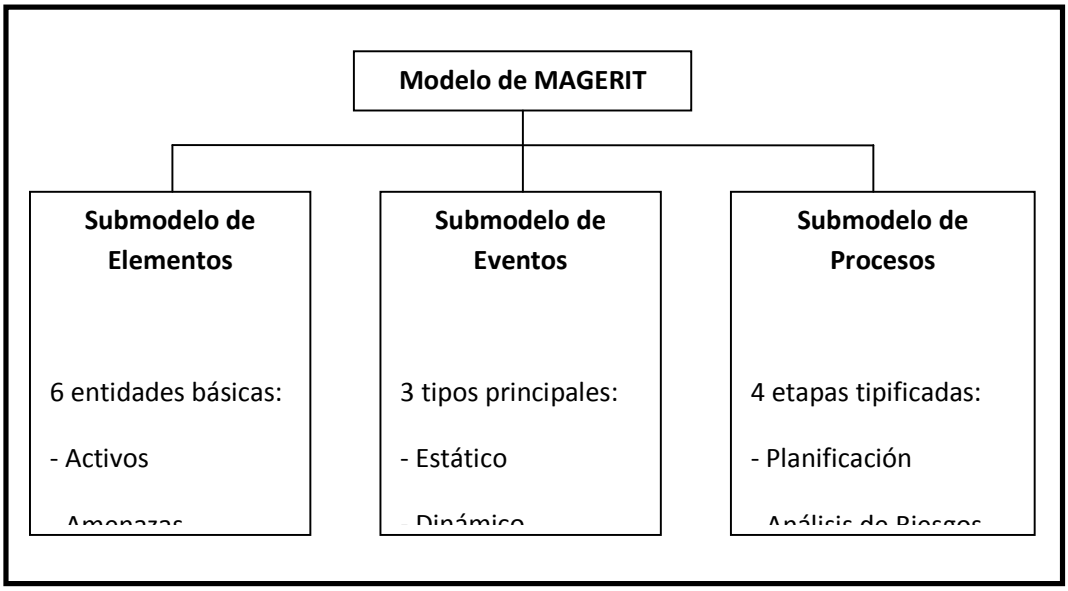


Figura 6.3 Modelo MAGERIT

El *Submodelo de Elementos* proporciona los "componentes" que el *Submodelo de Eventos* va a relacionar entre sí y con el tiempo, mientras que el *Submodelo de Procesos* será la descripción funcional ("el esquema explicativo") del proyecto de seguridad a construir.

El submodelo de procesos de MAGERIT comprende 4 etapas (así como se muestra en la figura 6.4):

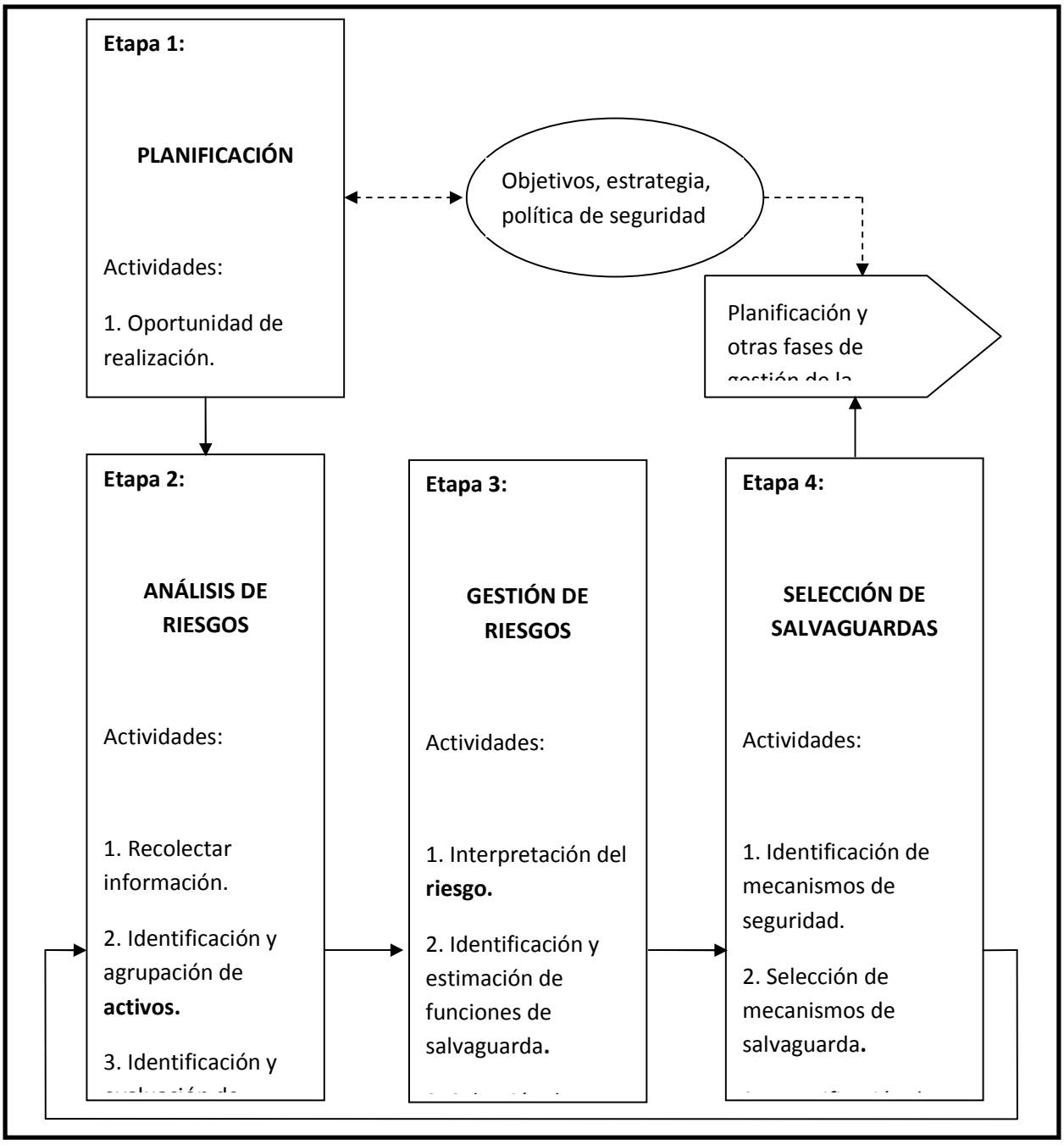


Figura 6.4 Etapas del Submodelo de procesos MAGERIT

1. **Planificación del Proyecto de Riesgos:** Como consideraciones iniciales para arrancar el proyecto de Análisis y Gestión de Riesgos (AGR), se estudia la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el ámbito que abarcará, planificando los medios materiales y humanos para su realización e inicializando el propio lanzamiento del proyecto.
2. **Análisis de riesgos:** Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable.
3. **Gestión de riesgos:** Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.
4. **Selección de salvaguardas:** Se prepara el plan de implantación de los mecanismos de salvaguarda elegidos y los procedimientos de seguimiento para la implantación. Se recopilan los documentos del Análisis y Gestión de Riesgos (AGR), para obtener los documentos finales del proyecto y realizar las presentaciones de resultados a diversos niveles.

Para lograr construir proyectos específicos de seguridad, MAGERIT posee interfaces de enlace con METRICA v2.1. MAGERIT permite añadir durante el desarrollo del sistema, la consideración de los requerimientos de seguridad, sin interferir en los procedimientos de Métrica, pero utilizándolos para identificar y documentar los procedimientos y productos de aseguramiento.
Estas interfaces tienen ventajas inmediatas, cómo: analizar la seguridad del sistema antes de su desarrollo así como la incorporación de defensas antes de completarlo (lo que es más barato y efectivo) y controlar su consistencia a lo largo de todo el ciclo de vida del Sistema.

Tipos de Técnicas usadas en MAGERIT

Cada una de las tareas del Submodelo de Procesos en la Guía de Procedimientos indica las técnicas empleadas para realizarla. MAGERIT tipifica las técnicas recomendadas como: Técnicas Comunes con METRICA v2.1 y con EUROMÉTOCO – Técnicas características

de MAGERIT, tales como matriciales, algorítmicas y de lógica difusa – Técnicas Complementarias.

MAGERIT consta de 7 guías:

1. **Guía de Aproximación:** Presenta los conceptos básicos de seguridad de los sistemas de información, con la finalidad de facilitar su comprensión por personal no especialista y ofrece una introducción al núcleo básico de MAGERIT, constituido por las Guías de Procedimientos y de Técnicas.
2. **Guía de Procedimientos:** Representa el núcleo del método que se completa con la Guía de Técnicas. Ambas constituyen un conjunto autosuficiente, puesto que basta su contenido para comprender la terminología para realizar el Análisis y Gestión de Riesgos de cualquier sistema de información.
3. **Guía de Técnicas:** Proporciona las claves para comprender y seleccionar las técnicas más adecuadas para los procedimientos de análisis y gestión de riesgos de seguridad de los sistemas de información.
4. **Guía para Responsables del Dominio Protegible:** Explica la participación de los directivos "responsables de un dominio" en la realización del análisis y gestión de riesgos de aquellos sistemas de información relacionados con los activos cuya gestión y seguridad les están encomendados.
5. **Guía para Desarrolladores de Aplicaciones:** Está diseñada para ser utilizada por los desarrolladores de aplicaciones y está íntimamente ligada con la Metodología de Planificación y Desarrollo de Sistemas de Información, Métrica v2.1
6. **Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos:** La interfaz para intercambio de datos posibilita que un usuario de MAGERIT establezca la comunicación con otras aplicaciones y sistemas facilitando la incorporación de sus productos a la herramienta MAGERIT y viceversa.
7. **Referencia de Normas legales y técnicas:** Lista de normas en materia de seguridad.

EBIOS (Expresision des Besoins et Identification des Objectifs de Sécurité - Expresión de las necesidades e identificación de los objetivos de seguridad): El método EBIOS es una herramienta de gestión de riesgos para los sistemas de seguridad informática, fue creada por la Dirección Central de Seguridad de los Sistemas de Información de Francia DCSSI.

El método EBIOS permite tratar los riesgos relativos a la seguridad de los sistemas de información (SSI), facilita la comunicación dentro y fuera del organismo para contribuir al proceso de la gestión de los riesgos SSI y ayuda a la toma de decisiones.
Este método toma en cuenta todas las entidades técnicas (software, hardware, redes) y no técnicas (organización, aspectos humanos, seguridad física).

Las características de EBIOS son:

- Es compatible con normalizaciones internacionales.
- Es utilizado para estudiar tanto sistemas por diseñar como sistemas ya existentes.
- Presenta y describe los tipos de entidades, métodos de ataque, vulnerabilidades, objetivos de seguridad y requerimientos de seguridad.

Los pasos del método EBIOS son:

1. **Estudio del contexto:** Durante este proceso se realiza un análisis de los activos de la organización, estos pueden ser distintos tipos como: hardware, software, redes, personal, entre otros.
2. **Expresión de las necesidades de seguridad:** En este proceso se realiza un estudio de las necesidades de seguridad para los activos determinados en el paso anterior.
3. **Estudio de las amenazas:** Al considerar que cada organismo se encuentra expuesto a diversos peligros, es importante realizar un estudio de las amenazas y vulnerabilidades a las que se encuentra expuesta la organización.
4. **Expresión de los objetivos de seguridad:** Este proceso consiste principalmente en cubrir las vulnerabilidades a las que la entidad se encuentra expuesta, es decir disminuir los riesgos.

5. **Determinar los requerimientos de seguridad:** Durante este proceso el equipo encargado del desarrollo del sistema de seguridad informática será el responsable de determinar las funcionalidades de seguridad esperadas, así como también el cumplimiento de los objetivos de seguridad.

CRAMM (Risk Analysis and Method Management): Es una metodología de análisis de riesgos desarrollada en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones (CCTA). Comenzó a desarrollarse en la década de 1980. En la figura 6.5 se muestra el modelo de análisis y gestión de riesgos de CRAMM el cual consiste en:

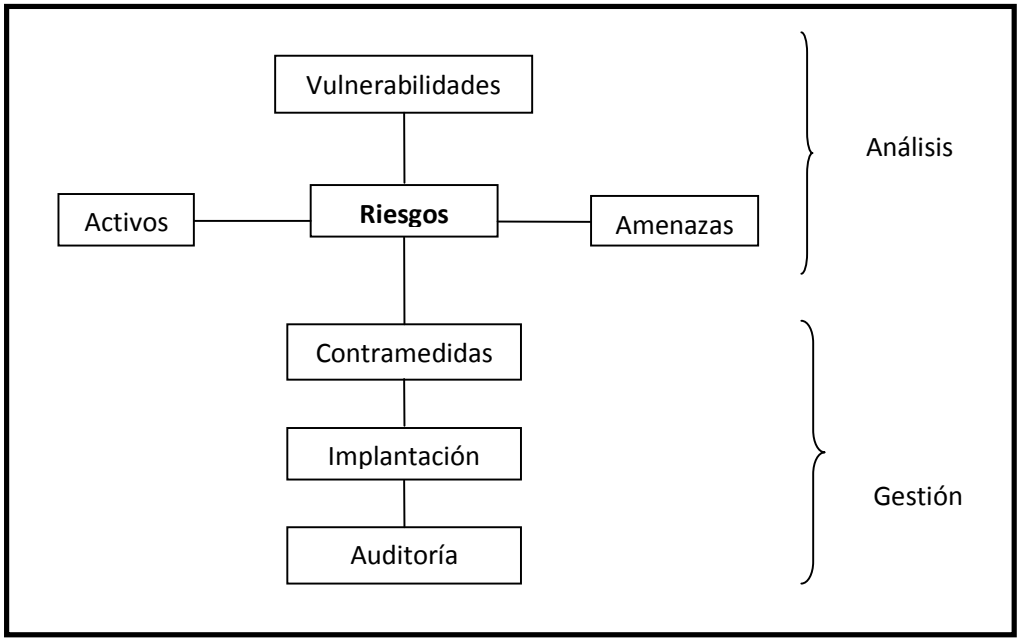


Figura 6.5 Modelo de análisis y gestión de riesgos de CRAMM

Uno de los aspectos principales de CRAMM es el soporte que proporciona la herramienta informática con una base de datos de:

- Más de 400 tipos de activos
- Más de 25 tipos de impacto
- 38 tipos de amenaza
- 7 tipos de medida del riesgo
- Más de 3,500 salvaguardas

CRAMM soporta 3 tipos de revisiones:

- CRAMM Express
- CRAMM Expert
- BS7799

Adicionalmente existen variantes para la gestión de riesgos en proyectos de desarrollo, con una interfaz al ciclo de vida estándar utilizado por la Administración Pública británica: SSADM (Structured System Analysis and Design Method).
La metodología CRAMM define tres fases para la realización del análisis de riesgos.

Fase 1: Establecimiento de objetivos de seguridad

Esta fase consiste en llevar a cabo los siguientes aspectos.

- Definir el alcance del estudio.
- Definir el valor de la información entrevistando a los usuarios sobre los impactos potenciales para el negocio que podrían producirse por la indisponibilidad, destrucción, divulgación o modificación.
- Identificar y evaluar los activos físicos que forman parte del sistema.
- Identificar y evaluar los activos de software que forman parte del sistema.

Fase 2: Análisis de riesgos

Consta de:

- Identificar y valorar el tipo de nivel de las amenazas que pueden afectar al sistema.
- Valorar las vulnerabilidades de los sistemas ante las amenazas identificadas.
- Combinar las valoraciones de amenazas y vulnerabilidades para calcular la medida de los riesgos.

Fase 3: Identificación y selección de salvaguardas

Los principales productos de la metodología CRAMM son:

- Documento de inicio del proyecto.
- Informes de análisis de riesgos.

- Informes de gestión de riesgos, cimentados en una base de datos de más de 3,500 salvaguardas técnicas y organizativas.
- Plan de implantación.

Las principales actividades del proceso de análisis y gestión de riesgos CRAMM se resumen en la siguiente figura (6.6):

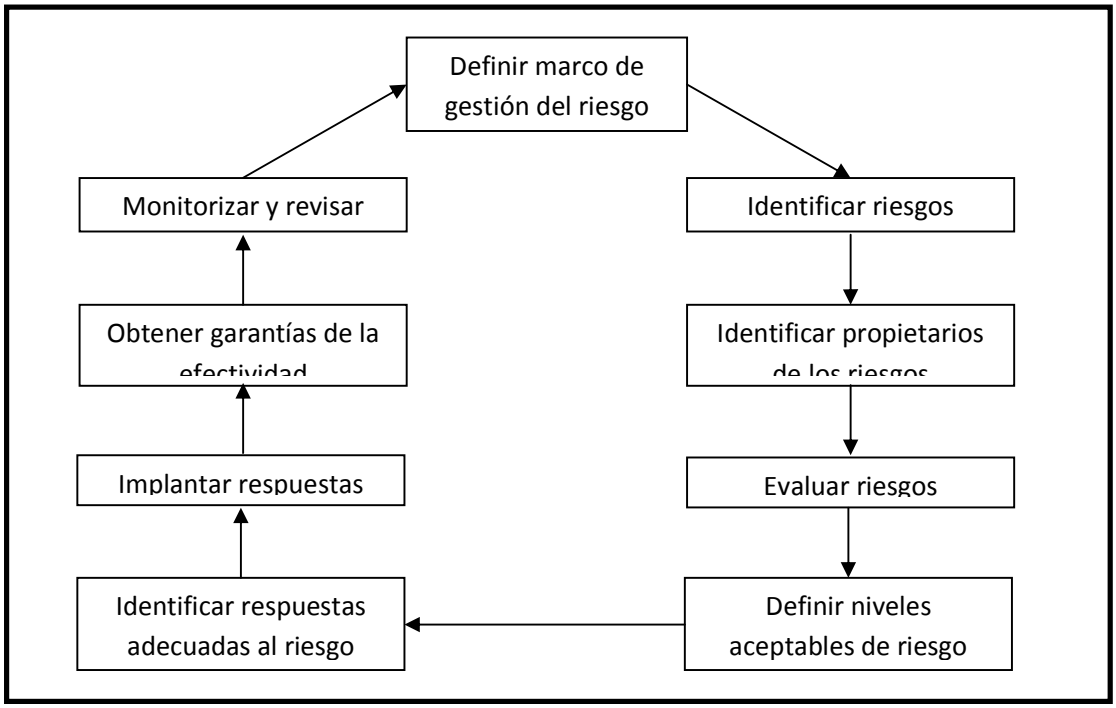


Figura 6.6 Principales actividades de análisis y gestión de riesgos de CRAMM

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*)**:** Es una técnica efectiva de evaluación de riesgos creada por la oficina de patentes y negocios de los Estados Unidos.

OCTAVE es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo, esta técnica está en contra de la consultoría enfocada en el campo tecnológico, que tiene como objetivo los riesgos tecnológicos y en los temas tácticos, OCTAVE se

enfoca en el riesgo organizacional y su objetivo principal son los temas relativos a la estrategia y a la práctica.

OCTAVE equilibra los siguientes aspectos:

- Riesgos operativos
- Prácticas de seguridad
- Tecnología

Lo cual permite a las compañías tomar decisiones de protección de información en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados a la información crítica.

Características:

- Es diferente de los análisis tradicionales enfocados a la tecnología
- Es autodirigido
- Flexible

Los objetivos de OCTAVE son:

- Permitir la comprensión del manejo de los recursos
- Identificación y evaluación de los riesgos que afectan la seguridad dentro de una organización.
- Exige llevar la evaluación de la organización y del personal de la tecnología de información.

Este método se enfoca en tres fases para examinar los problemas organizacionales y tecnológicos, los cuales son:

Fase I: Durante esta fase se identifica la información de la organización. Los procesos que se realiza en esta fase son:

- Establecer criterios de evaluación de impacto
- Identificar sus criterios de seguridad
- Identificar sus amenazas
- Analizar los procesos tecnológicos relacionados

Fase II: En esta fase se examina la infraestructura tecnológica y se realizan los siguientes procesos:

- Examinar rutas de acceso
- Analizar procesos tecnológicos

Fase III: Durante esta fase se realiza la identificación de los riesgos, así como también se realizan estrategias de mitigación y planes de protección. Los procesos que intervienen en esta fase son:

- Evaluar el impacto de las amenazas
- Evaluar la probabilidad de ocurrencia de amenazas
- Seleccionar formas de mitigación de riesgos
- Desarrollar planes de mitigación de riesgos

6.3 Herramientas de Seguridad

Las herramientas de seguridad informática son una parte fundamental para el desarrollo de cualquier sistema de seguridad de redes de computadoras, por ello es muy importante conocer los tipos de herramientas tanto de software como de hardware existentes y a su vez clasificarlos acorde a las necesidades de cada usuario. Si bien es cierto que a lo largo del tiempo, se han desarrollado diversas aplicaciones cuyo objetivo es prevenir y mitigar los posibles ataques a los que se están expuestos todos los días, desafortunadamente existen personas que desafían a las herramientas, logrando burlar la seguridad y cumplir sus objetivos. Por este y otros motivos se debe de procurar estar actualizados ante los nuevos avances tecnológicos y una forma para ayudar a lograrlo es incluir en el capítulo 7 titulado Herramientas de Seguridad los siguientes temas (**Monitoreo, Paswords, Auditoría, Criptografía, Código Malicioso, Escaneo, Filtrado, Detección de Intrusos y Autenticación),** los cuales se desarrollan a continuación:

6.3.1 Monitoreo

El término monitoreo de red describe el uso de un sistema que constantemente monitorea una red de computadoras para detectar sistemas lentos o en mal funcionamiento y que notifica al administrador de la red en caso de falla vía correo electrónico, beeper u otras alarmas. Sirven para el control sobre algunos eventos que van sucediendo en un sistema de computación, que puede ser desde un sistema aislado, hasta una red de computadoras muy compleja. Su principal objetivo es analizar los eventos conforme suceden a fin de detectar condiciones anómalas o indeseadas y generar las alarmas correspondientes.

Los aplicativos de monitoreo del estado de red permiten:

- **Revisar los signos vitales de la red en tiempo real:** Mientras un sistema de detección de intrusos monitorea una red de amenazas del exterior, un sistema de monitoreo de red vigila la actividad en la red en busca de problemas debidos a servidores, conexiones de red u otros dispositivos sobrecargados y/o fuera de servicio para informar al administrador de la red.

Existe un gran número de herramientas de monitoreo en el mercado y éstas se pueden dividir en dos tipos:

A. Herramientas de control y seguimiento de accesos: Estas herramientas permiten obtener información (mediante ficheros de trazas) de todos los intentos de conexión que se produzcan en el sistema o sobre otro que se indiquen, así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UDP.

Este tipo de herramientas permiten tener control sobre todos los paquetes que entran por la interfaz de red de la máquina: IP (TCP, UDP) e ICMP, o analizando paquetes a nivel de aplicaciones como:

- **Telnet:** Abre una sesión en una máquina remota.
- **FTP:** Transfiere archivos desde una máquina remota.
- **SMTP (Simple Mail Transfer Protocol):** Utilizado para enviar y recibir correo electrónico.

Estas herramientas pueden ser utilizadas junto con otras que permitan definir desde qué máquinas se permiten ciertas conexiones y de cuáles se prohíben.

Algunas de éstas pueden tener un doble uso, es decir, ofrecer protección ante posibles ataques, pero también podrían ser utilizadas para intentar comprometer sistemas. Por eso es importante que el uso de estas herramientas esté restringido de manera que el personal no autorizado no pueda utilizarlas de forma aleatoria y se oculte realmente un ataque. También podrán ser utilizadas para hacer seguimientos en la red cuando se sospeche que alguna de las máquinas en la red ha sido comprometida.

Sin embargo, estas herramientas son muy inseguras ya que a su paso por Internet existen programas que pueden identificar todo el flujo de información de manera textual desde una máquina hacia otra incluyendo el nombre y la contraseña del usuario. Para evitarlo, se crearon las siguientes herramientas:

- **Achilles:** Es una herramienta designada parar comprobar la seguridad de aplicaciones web. Achilles es un servidor Proxy que actúa como una persona en el medio (main in the middle) durante una sesión de http. Un Proxy de http típico para paquetes hacia y desde el explorador de web cliente y un servidor de web. Esta herramienta intercepta los datos en una sesión de http en cualquier dirección y le da al usuario la habilidad de alterar datos antes de ser transmitidos.
- **AirSnort:** Herramienta de crackeo del cifrado WEP de 802.11. Es una herramienta para LANs inalámbricas (WLAN) que recupera las llaves de cifrado. Fue desarrollada por el Shmoo Group y opera monitoreando pasivamente las transmisiones, computando la llave de cifrado cuando suficientes paquetes han sido recolectados.
- **Brutus:** Cracker de autenticación para redes. Este cracker es sólo para Windows, se extiende sobre servicios de red de sistemas remotos tratando de averiguar passwords utilizando un diccionario y permutaciones de éste. Soporta http, POP3, FTP, SMB, TELNET, IMAP, NTP, entre otros.

- **Cain & Abel:** Es una herramienta de recuperación de passwords para los sistemas operativos de Microsoft. Permite una fácil recuperación de varias clases de password, escuchando (sniffing) la red, crackeando los passwords cifrados utilizando ataques por diccionarios, decodificando passwords codificados (scrambled) y revelando cuadros de diálogo del tipo password.
- **Código Malicioso:** Existen herramientas generales que suelen brindar protección en "tiempo real" y otras contra determinado código malicioso (vacunas). También hay herramientas contra Spyware como el Norton Antivirus y Trend, Titanium/Enterprise.
- **DSniff:** Es un juego de herramientas de auditoría y pruebas de penetración de redes. Incluye dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf y webspy que monitorean pasivamente una red en busca de datos (passwords, e-mail, archivos, entre otros.)
- **Ethereal:** Es un analizador de protocolos de red para Unix y Windows. Permite examinar datos de una red viva o de un archivo de captura en algún disco.
- **Ettercap:** Es un interceptor sniffer registrador para LANs con Ethernet basado en terminals. Soporta direcciones activas y pasivas de varios protocolos.
- **Firewall:** software que se instala en una computadora la cual es el intermediario entre la red local (correspondiente a la organización) y la red externa que por lo general es Internet, aunque también pueden existir firewall entre diferentes redes dentro de una organización si así se desea.
- **Firewalk:** Analiza las respuestas a paquetes IP para determinar mapas de redes y filtros de listas de control de acceso (ACL) empleadas por gateways.
- **Fport:** Reporta todos los puertos TCP/IP y UDP abiertos en la máquina en la que se está ejecutando y muestra qué aplicación abrió cada puerto y sus aplicaciones asociadas.
- **GFI LANguard:** Esta herramienta escanea redes y reporta información como el nivel de "service pack" de cada máquina, faltas de parches de seguridad, recursos compartidos, puertos abiertos, servicios / aplicaciones activas en la computadora, datos del registro, passwords débiles, usuarios y grupos; y más.

- **Hping2:** Esta herramienta ensambla y envía paquetes de ICMP/UDP/TCP hechos a medida y muestra la respuesta. Fue inspirado por el comando ping, pero ofrece mucho más control sobre lo enviado.
- **IDS (Intrusion Detection System):** Sistema para detectar intrusiones al sistema[46].
- **ISS Internet Scanner:** Esta herramienta consiste en la evaluación de vulnerabilidades a nivel de Aplicación.
- **John the Ripper:** Su propósito principal es detector passwords.
- **Kismet:** Es un sniffer para redes inalámbricas, detecta bloques de IP automáticamente por medio de paquetes UDP, ARP y DHCP.
- **Kerberos:** es un protocolo de seguridad para realizar servicios de autenticación en la red, usa la criptografía basada en claves secretas para proporcionar la seguridad de las contraseñas en la red, por consiguiente, el cifrado de contraseñas con kerberos ayuda a evitar que los usuarios no autorizados intercepten contraseñas en la red, esto representa un método de seguridad del sistema. Es un proceso en el que diferentes elementos colaboran para conseguir identificar a un cliente que solicita un servicio ante un servidor que lo ofrece; asegura que las contraseñas nunca se envíen de manera clara a través de la red. Un uso correcto de kerberos erradica la amenaza de analizadores de paquetes que interceptan contraseñas en la red. Cada usuario tiene una clave y cada servidor también, por lo tanto, se tiene una base de datos que las contiene a todas. En el caso de ser de un usuario, su clave se deriva de su contraseña y está cifrada, mientras que en el caso del servidor, la clave se genera aleatoriamente. Los servicios de red que requieren autenticación y los usuarios que requieren estos servicios, se deben registrar con kerberos. Como éste conoce todas las claves privadas, puede crear mensajes que convencen a un servidor de que un usuario es realmente quien dice ser y viceversa.
- **NBTScan:** Recolecta información de NetBIOS de redes de Windows.
- **Netcat:** Es una herramienta para Unix que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP.

[46] Un intruso es alguien que trata de destruir el sistema desde dentro o darle un mal uso. Por darle un mal uso se entiende desde robar información confidencial hasta usar un correo para enviar correo spam.

- **Netfilter:** Es un filtro de paquetes el cual es implementado en el Kernel de Linux estándar.
- **Network Stumbler:** Es utilizada para encontrar "acces point" inalámbricos abiertos ("wardriving").
- **NGrep:** Busca y muestra paquetes.
- **Nikto:** Es un escáner de web de mayor amplitud. Busca más de 2000 archivos / CGIs potencialmente peligrosos y problemas en más de 200 servidores.
- **Nmap:** Existe para el escaneo de puertos, éste permite a los administradores de sistemas el escaneo de grandes redes para determinar qué servidores se encuentran activos y qué servicios ofrecen.
- **N-Stealth:** Escáner de servidores Web.
- **NTop:** Es un monitor de uso de tráfico de red.
- **OpenSSH (Open secure shell):** Se encarga de cifrar el tráfico incluyendo las contraseñas, para eliminar de un modo efectivo el espionaje, los secuestros de las conexiones y otros ataques a nivel de red, de tal manera que permite realizar la comunicación y transferencia de información de forma cifrada pues proporciona fuerte autenticación sobre un medio inseguro. OpenSSH ofrece amplias posibilidades para la creación de túneles seguros, aparte de una variedad de métodos de autenticación.
- **Parches (patch):** Es conveniente su colocación en el sistema, ya que diariamente surgen nuevos ataques a través de agujeros no protegidos por el sistema y al poner estos parches se pueden contrarrestar las posibles incursiones de los atacantes informáticos además de que éstos permiten actualizar y mejorar la operatividad del sistema.
- **Passwords:** Se utilizan para mejorar el tratamiento de los passwords, brindando un mayor grado de seguridad a los recursos de los usuarios. Una posible clasificación es la siguiente:
    - **De Crackeo:** Ayuda a la detección de passwords débiles.
    - **Generadores:** Ayudan a obtener passwords buenos. Se basan en distintos algoritmos.
    - **Ocultamiento:** Ayuda a esconder los archivos de passwords del sistema.

- **PEM (Privacy Enhaced Mail):** Da soporte a la criptografía, autenticación e integridad de mensajes de correo electrónico ya que permite cifrar de manera automática los mensajes antes de enviarlos. PEM realiza las siguientes funciones:
    - Especifica los formatos de mensajes para pedir y revocar certificados.
    - Especifica la jerarquía de las autoridades certificadoras (AC).
    - Especifica la jerarquía de los algoritmos de criptografía.
- **Portsentry:** Programa que cuenta con un archivo de los puertos más vulnerables del sistema, también se pueden agregar a esa lista otros que no se consideran pertinentes para la seguridad del sistema, esta herramienta identifica si alguien quiere entrar por alguno de esos puertos impidiéndole la entrada.
- **SAINT (Security Administrator's Integrated Network Tool):** Herramienta de red integrada para el administrador de seguridad. Funciona únicamente sobre UNIX.
- **Sam Spade:** Herramienta de consulta de redes.
- **SARA:** Asistente de Investigación para El Auditor de Seguridad (Security Auditor's Researchs Asistant). Es una herramienta de evaluación de vulnerabilidades.
- **Sniffer:** Herramienta para la revisión de una red, se puede observar en forma clara conexiones no encriptadas, también permite verificar varios servicios como el correo por su puerto 25, la web por su puerto 80 y todos los servicios que se desean revisar en cada momento.
- **Snort:** Es un sistema de detección de intrusos de red capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP.
- **SSL (Secure socket layer):** Sistema de protocolos de carácter general diseñado en 1994 por la empresa Netscape Communications Corporation, está basado en la aplicación conjunta de criptografía simétrica, criptografía asimétrica, certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet, es idóneo para transferir información personal o relacionada con transacciones financieras a través de Internet de forma segura y privada. SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socket, de forma transparente al usuario y a las aplicaciones que lo usan. Actualmente es el estándar de comunicación segura en los navegadores más importantes como Netscape Navigator e Internet Explorer.

- **SuperScan:** Es un escáner de puertos de TCP. Puede manejar escaneos por ping y escaneo de puertos utilizando rangos de IP específicos.
- **THC-Amap:** Es un escáner de identificación de aplicaciones y servicios.
- **Tripwire:** Monitor de la integridad de los archivos, esta herramienta rastrea cambios en los permisos de los archivos y ligas, tamaños en archivos, tamaños en directorios y cambios en los identificadores de grupos (groupid) y usuarios (userid).
- **TCPDump / WinDump:** Es un analizador de paquetes de red basado en texto. Puede ser utilizado para mostrar los encabezados de los paquetes en un interfaz de red que concuerden con cierta expresión de búsqueda. Se puede utilizar para rastrear problemas en la red o para monitorear actividades de la misma.
- **Whisker/Libwhiske:** Whisker es un escáner que permite poner a prueba servidores de HTTP con respecto a varios agujeros de seguridad conocidos, particularmente, la presencia de peligrosos scripts que utilicen CGI.
- **Windows Privacy Tools (Herramientas de privacidad para Windows):** Colección de aplicaciones multilingües para facilitar el cifrado de contenidos –como el correo electrónico–, la firma digital y la gestión de claves. Se basa en GnuPG, que es compatible con aplicaciones que soportan OpenPGP (como PGP) y además es gratis para uso comercial y personal, bajo la licencia GPL.
- **XProbe2:** Herramienta que sirve para determinar el sistema operativos de un host remoto.

B. Herramientas que verifican la integridad del sistema

Estas herramientas ayudan a proteger el sistema. Algunas se basan en el chequeo a los ficheros y otras alertan de posibles modificaciones de ficheros y de programas “sospechosos” que puedan estar ejecutándose en la máquina de manera oculta, algunas de estas herramientas son:

- **Crack:** Es una herramienta que consiste únicamente en crackear passwords.
- **Chklastlog:** Software para detectar modificaciones en el archivo de log para Unix.
- **Chkwtmp:** Software para detectar modificaciones en el archivo wtmp de Unix.

- **Cmp (Check Promiscuous Mode):** Este programa se encarga de revisar la interfaz de red de la máquina descubriendo si está siendo utilizada en modo promiscuo (escuchando todo el tráfico de la red).
- **COPS (Computer Oracle and Password System):** Esta herramienta se encarga de revisar las posibles vulnerabilidades y agujeros de seguridad existentes.
- **Ifstatus:** Es una herramienta que facilita de forma gráfica y en tiempo real, lo que está haciendo la tarjeta de real.
- **LSOF (List Open Files):** Es una herramienta de diagnostico específica de UNIX, la cual lista la información acerca de cualquier archivo abierto por procesos que estén actualmente ejecutándose en el sistema. También puede listar sockets de comunicaciones abiertos por cada proceso.
- **Noshell:** Este software permite al administrador obtener información adiciona sobre intentos de conexión a cuentas canceladas en una máquina.
- **Osh (Operator Shell):** Este software es de dominio público, es una shell restringida que permite indicar al administrador mediante un archivo de datos qué comandos puede ejecutar cada usuario.
- **Spar:** Software de dominio público diseñado por CSTC (Computer Security Technology Center) que realiza una auditoría de los procesos del sistema, mucho más flexible y potente que el comando lastcomm de UNIX.
- **Tiger:** Es un software que está conformado por un conjunto de shell scripts y código C que chequean el sistema para detectar problemas de seguridad de forma parecida a COPS.

Algunos productos son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **SolarWinds:** Ayuda a empresas de cualquier tamaño a monitorizar y gestionar sus redes corporativas con una eficiencia en costos, con productos fáciles de usar, rápidos de implementar y muy efectivos. (www.solarwinds.net)
- **Iris:** El servicio de seguridad de RedIRIS tiene como finalidad la detección de problemas que afecten a la seguridad de las redes de centros de redIRIS, así

como la actuación coordinada con dichos centros para poner solución a estos problemas. También se realiza labor preventiva, avisando con tiempo de problemas potenciales, ofreciendo asesoramiento a los centros, organizando actividades de acuerdo con los mismos y ofreciendo servicios complementarios. www.eeye.com

- **Ethereal:** Es una potente herramienta que incluye todas las funciones necesarias para ejecutar análisis exhaustivos de protocolos en redes Ethernet. www.ethereal.com
- **MS Operations Manager:** Es una herramienta de monitoreo que permite la administración de manera eficaz y eficiente de las alarmas y eventos que se realizan en un sistema que se esté controlando, presentando una interfaz de usuario muy amigable, integrándose apropiadamente con el Directorio Activo y permite fusionarse adecuadamente con otras herramientas de administración y monitoreo de otros fabricantes. www.microfosft.com
- **Core Wisdom:** Es un conjunto de herramientas diseñadas para facilitar la auditoría segura de sistemas informáticos. Esta solución centraliza y garantiza la integridad de la información del sistema y optimiza la auditoría, procesando y representando la información en diferentes modos gráficos. La suite posibilita en análisis sobre información histórica al mismo tiempo que reproduce los eventos en tiempo real, permitiendo alta disponibilidad de los sistemas. http://www1.corest.com/

6.3.2 Auditoría

La utilización de herramientas de auditoría permite la detección de puntos débiles en el sistema, así como el seguimiento de determinadas actividades y/o de usuarios. Así mismo, brinda un panorama acerca del perfil de funcionamiento del sistema en condiciones normales.

Así, este tipo de herramientas sirven para verificar en diferido el funcionamiento normal de un sistema o la ocurrencia de determinados hechos basándose en información recolectada con tales fines. Las más comunes son aquellas que hacen el análisis de los archivos de logs, tanto del sistema operativo como de aplicaciones específicas.

Existen otras herramientas, tales como los antivirus, que proveen sus propias funcionalidades de auditoría. En ocasiones, el resultado producido por las herramientas de auditoría sirve como entrada a otros sistemas de protección, como es el caso de los IDS y de los escaneadores de vulnerabilidades.

Algunas de las herramientas más comunes son:

- **Bastille:** Un script de fortalecimiento de seguridad Para Linux, MacOS X, y HP-UX.
- **Cheops / cheops-ng:** Nos provee de una interfaz simple a muchas utilidades de red, mapea redes locales o remotas e identifica los sistemas operativos de las máquinas.
- **Crack / Cracklib:** El clásico cracker de passwords locales de Alec Muffett.
- **Dig:** Una útil herramienta de consulta de DNS que viene de la mano con Bind.
- **Etherape:** Monitor de red gráfico para Unix basado en etherman.
- **Fping:** Programa para el escaneo con ping en paralelo.
- **IpTraf:** Software para el monitoreo de redes de IP.
- **LibNet:** Es una API (toolkit) de alto nivel permitiendo al programador de aplicaciones construir e inyectar paquetes de red.
- **OpenBSD:** El sistema operativo preventivamente seguro.
- **Shadow Security Scanner:** Una herramienta de evaluación de seguridad no libre
- **Tcpreplay:** Herramienta para reproducir (replay) archivos guardados con tcpdump o con snoop a velocidades arbitrarias.
- **TCPTraceroute:** Es una implementación de traceroute que utiliza paquetes de TCP.

- **Tcp wrappers:** Su función radica en que autentica las redes, es decir, reconoce que la Ip de una red en realidad pertenece a dicha red. Esto se debe a que alguien que sabe la aceptación de una Ip para ingresar a un sistema, puede poner en una red inventada esa Ip –a esto se le llama spoofing– y así ingresar a cierto sistema.
- **pwdump3:** Permite recuperar las hashes de passwords de Windows localmente o a través de la red aunque syskey no esté habilitado.
- **The Coroner's Toolkit (TCT):** Colección de herramientas orientadas tanto a la recolección como al análisis de información forense en un sistema Unix.
- **Visual Route:** Obtiene información de traceroute/whois y la grafica sobre un mapa del mundo.
- **Winfingerprint:** Escáner de enumeración de Hosts/Redes para Win32.

Algunos productos son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **BindView:** Es una herramienta que ofrece el acceso y análisis de los datos fundamentales para el administrador de la red de forma sencilla y gráfico desde un único interface. www.bindview.com
- **DumpSec:** Es un programa de auditorías de seguridad para Microsoft Windows NT/XP/200X. vuelca los permisos (DACL –Lista de control de acceso direccional-) y la configuración de auditoría (SACL –Auditoría de acceso a objetos-) para el sistema de archivo, registro, impresoras y recursos compartidos en un formato conciso, legible, de modo que los agujeros en la seguridad del sistema son evidentes. www.somasoft.com

6.3.3 Criptografía

Las herramientas criptográficas son usadas en diferentes ambientes o partes de los sistemas como:

- Contraseñas
- File System

- Canales de comunicación
- Correo electrónico
- PKI

En general soportan varios algoritmos de cifrado.

Algunos productos son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **GNUPG**: Programa de encriptación que ayuda a proteger la información de curiosos y otros riesgos.
- **PGP (Pretty Good Privacy):** Aplicación ampliamente utilizada en todo el mundo, sobre todo por usuarios particulares, ya que se trata de un programa de cifrado de datos que incluye múltiples funciones de seguridad adicionales y de gestión de claves, permite intercambiar archivos y mensajes con seguridad y comodidad. Está basado en un conjunto de comandos muy sencillos y en la criptografía de clave pública. PGP puede utilizarse para firmar un mensaje, como un certificado de autenticidad y para enviar archivos a través de correo electrónico codificados en formato ASCII, esto proporciona servicios de autenticación y confidencialidad, tanto para el correo electrónico como para el almacenamiento de archivos. (www.pgp.com)
- **Steganos:** Herramienta diseñada para proteger la computadora de los diferentes códigos maliciosos que atacan desde Internet. (www.steganos.com)
- **Tripwire:** Esta herramienta se utiliza para comprobar la integridad de archivos y directorios. Ayuda a administradores y usuarios de sistemas monitoreando alguna posible modificación en algún set de archivos. Si se usa regularmente en los archivos de sistema, tripwire puede notificar a los administradores del sistema, si algún archivo fue modificado o reemplazado, para que se puedan tomar medidas de control de daños a tiempo. (www.tripwire.org)

6.3.4 Escaneo

Estas herramientas basan su funcionamiento en realizar un "recorrido" a través de un conjunto de host (un rango de direcciones IP, un dominio, entre otros.) para revisar sus estatus de seguridad. En este barrido, interrogan a cada host respecto a cómo está preparado ante las vulnerabilidades conocidas.

Un tipo de herramienta muy utilizada por los administradores de redes es el escáner de puertos, éste se encarga de revisar e identificar cuáles puertos están abiertos en un host para detectar los servicios que están disponibles.

Algunos productos son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **GFILanguard:** Es un escáner de red y de seguridad. Escanea la red y puertos para detectar, evaluar y corregir vulnerabilidades de seguridad con mínimo esfuerzo administrativo.(www.gfi.com)
- **Nessus:** Herramienta de evaluación de seguridad "Open Source" → de mayor renombre. Nessus es un escáner de seguridad remoto para Linux, BSD, Solaris y otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX y texto ASCII; también sugiere soluciones para los problemas de seguridad. (www.nessus.org)
- **Retina:** Su función es escanear todos los host en una red y reportar cualquier vulnerabilidad encontrada.(www.eeye.com)

6.3.5 Filtrado

Son herramientas que funcionan bajo reglas para permitir o denegar tráfico de acuerdo a criterios tal como direcciones IP, puertos y protocolos entre otros.

La mayoría de estas herramientas funcionan de modo automático a partir de las reglas configuradas, pero también existen otras de funcionamiento manual, las cuales ante determinadas alertas y con base en las políticas de seguridad de la organización hacen que el administrador decida si deja pasar o no, cierta conexión. Las herramientas más comunes son los firewalls.

Firewall

Entre las comunicaciones que pueden protegerse mediante un firewall están las que se muestran en la figura 6.7.

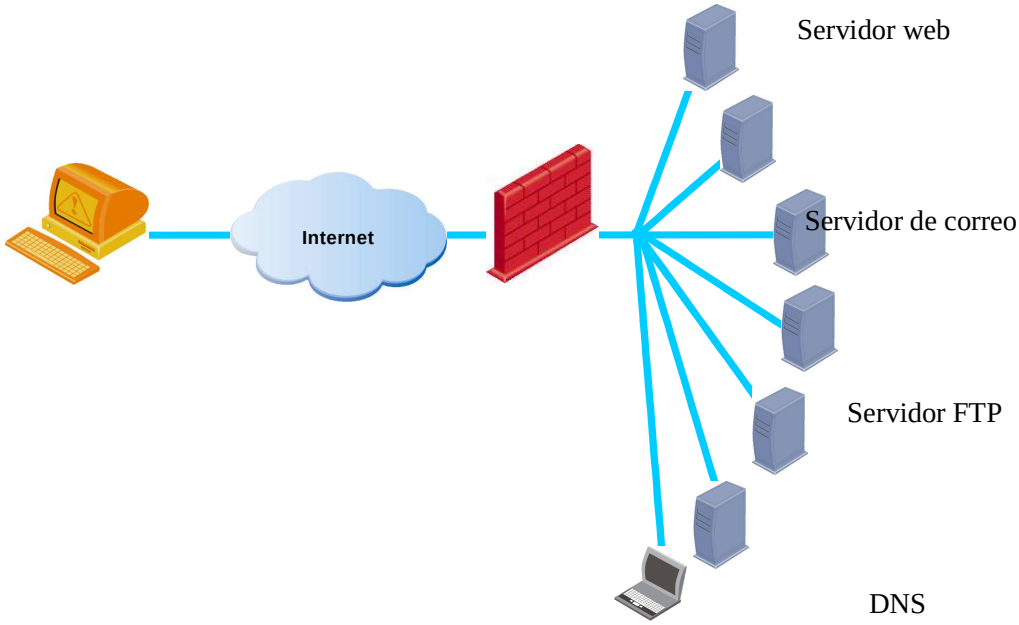


Figura 6.7 Esquema de protección mediante un firewall

Los firewalls funcionan bajo alguna de las dos siguientes filosofías:

- Dejar pasar a todas las redes exceptuando a las que no se desea.
- Negar el acceso a todas las redes y sólo permitir a las que se desea.

La selección de la filosofía también depende directamente de las necesidades identificadas y de las políticas que al respecto (control de acceso) se hayan escrito.
En la máquina donde se instale el firewall sólo debe existir ese software activo y no usarla para otras aplicaciones, ya que el firewall sólo es el puente de comunicación entre las redes local y externa y no debe haber otro trabajo realizándose ni ninguna otra información guardada, ya que en caso de que llegara a ser accedida por alguna persona no autorizada, sólo podría dañar al firewall, el cual no contiene información importante de la organización y podría reponerse de inmediato tapando el agujero por donde se infiltró el perpetrador.

Un Firewall o cortafuegos es una combinación de elementos de hardware y software que se ubica principalmente entre dos redes, tal como una red interna y un ISP (Internet Service Provider) así cómo se muestra en la figura 6.8.

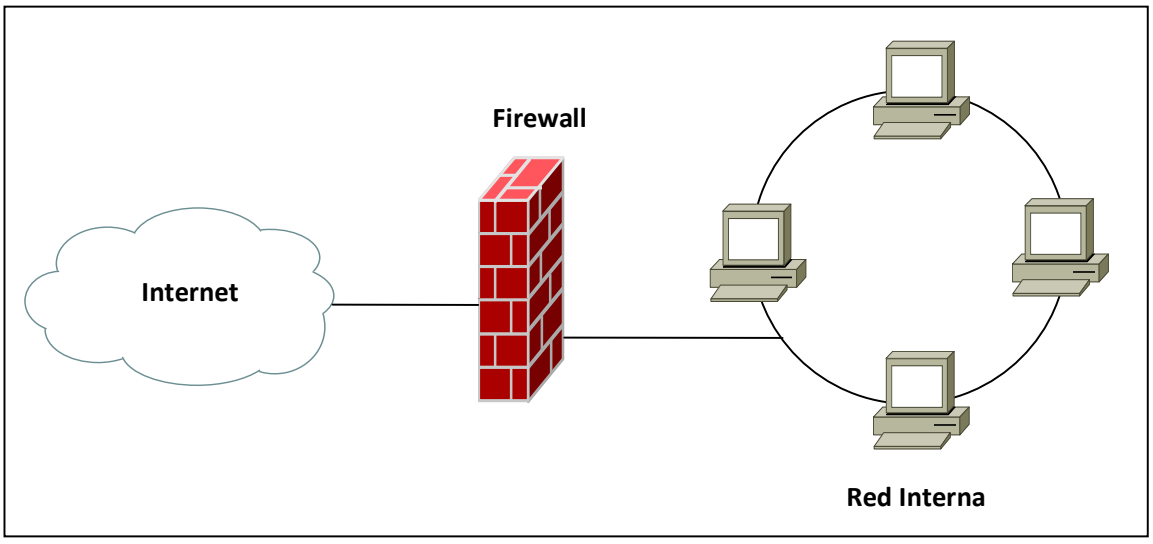


Figura 6.8 Firewall

Sin embargo es necesario hacer notar que también se puede ubicar dentro de una misma red para separar segmentos restringidos donde se procesa o se ubican los servidores con la información sensible de la organización.

El Objetivo del firewall es proteger a la red interna, evitando que usuarios externos no autorizados tengan acceso a la red. También se puede usar para que los usuarios internos no envíen tráfico destinado a determinados receptores fuera de la red.

Para que un firewall sea eficiente se deben garantizar los siguientes aspectos:

- Que todo el tráfico entrante y saliente pase a través de él.
- Que deje pasar sólo el tráfico autorizado por la política de seguridad (se implementa mediante reglas).
- Que sea inmune a ataques dirigidos a él.

Existen básicamente 2 tipos de firewall:

a) Packet filter: El filtrado se realiza para cada paquete que entra o sale de la red. Las reglas de filtrado se basan en:

- Dirección IP origen
- Dirección IP destino
- Puerto Origen
- Puerto Destino

Este tipo de filtrado es estático, para realizar algún cambio sobre éste se deben de cambiar las reglas. Algunas ventajas de packet filter son:

- Simple: Se puede implementar en routers con ACL
- Bajo costo
- Alto rendimiento

Desventajas:

- **Filtrado estático:** Para cambiar algo, se deben de cambiar las reglas.
- **Susceptibles de spoofing**

b) Statefull inspection: Posee una especie de “filtrado inteligente”. El firewall permite o deniega sesiones (entrantes o salientes) tomando en cuenta el estado de las conexiones a partir del análisis de cada uno de los paquetes para obtener información acerca de la sesión. El filtrado se hace sobre la sesión. Algunas ventajas son:

- Filtrado dinámico
- Bajo costo
- Más seguro que packet filter
- Buena capacidad de jogging

Algunas desventajas son:

- No todos los routers lo soportan
- La configuración de reglas es más compleja que el packet filter

Por lo tanto se puede concluir que los firewalls de filtrado:

- Mejoran la seguridad de la red interna frente a los ataques externos.
- No proveen autenticación de usuarios: si se requiere, se deberá implementar en algún servidor de la red interna.
- La configuración de las reglas de filtrado es una tarea bastante compleja.
- Permiten conexiones directas end-to-end.
- Una debilidad: una vez que un atacante ganó acceso a la red interna, podrá acceder directamente a cualquier host con vulnerabilidades (principalmente los que están mal configurados.)
- No brindan protección a ataques internos (excepto que se use algún firewall interno).
- No tienen capacidad para evitar ataques que se basan en servicios autorizados.

Proxy

El proxy es un servidor conectado normalmente al servidor de acceso de la www de un proveedor de acceso que va almacenando toda la información que los usuarios reciben de la web, por lo tanto, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información del servidor proxy en lugar del servidor real.[47]

El proxy funciona en un host ubicado como "conector" de una red interna con servidores externos a la misma. Los usuarios de la red interna solicitan servicios de

[47] http://www.definicion.org/proxy

Internet a través del Proxy y éste se ocupa de establecer una nueva conexión hacia el sistema destino, así como se muestra en la siguiente figura 6.9.

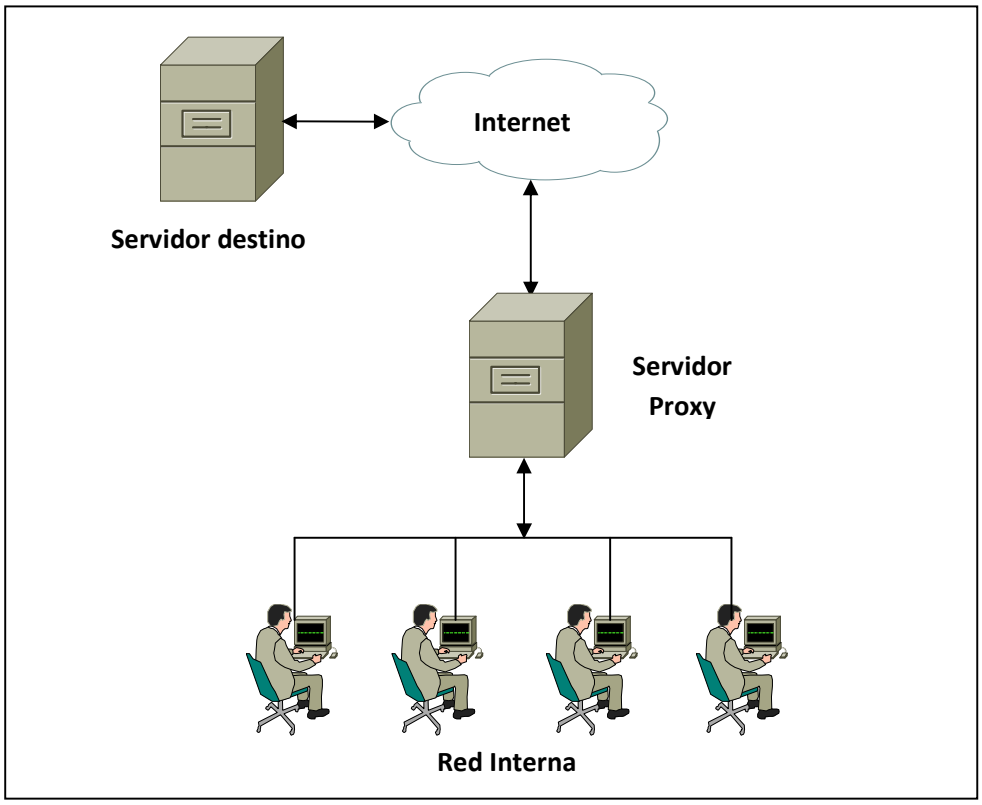


Figura 6.9 Proxy

Algunas características del Proxy:

- Emplea software para capturar, analizar y realizar la inspección de seguridad para cada conexión en cada protocolo.
- Cuando aprueba un requerimiento lo redirige hacia el servidor externo que corresponda, es decir, que actúa como servidor y como cliente.
- Para los clientes, el Proxy es transparente.
- Tiene la capacidad de autenticar usuarios finales.
- Suministran servicios de buffer: por ejemplo, pueden mantener un conjunto de páginas almacenadas en su disco local de modo que si son nuevamente referenciadas por algún cliente, la conexión se pueda establecer rápidamente sin necesidad de acceder al exterior para traerlas.

- Pueden monitorear lo que está pasando en la red interna.

Ventajas del Proxy:

- Proporcionan un buen nivel de seguridad.
- No permiten conexiones directas end-to-end.
- Tienen un buen registro de actividad.
- Proveen autenticación de usuarios.
- Son simples de administrar.

Desventajas del Proxy:

- Tienen un alto requerimiento de CPU.
- Requerimiento de un Proxy por cada protocolo (Proxy de aplicación).

La implementación de un firewall en una organización dependerá de varios aspectos, principalmente del grado de seguridad deseado en función de las características de la empresa y de un adecuado análisis de costos.

Muchas veces no cubren la totalidad de los equipos de la red interna (alguna conexión que "burla" los mecanismos de protección).
Algunos productos de firewall's son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **BlackIce:** Proporciona un sólido Firewall que detecta, informa y bloquea eficazmente los intentos de intrusión.
- **Firewall-1:** Esta herramienta incorpora una nueva arquitectura dentro del mundo de los cortafuegos: la inspección con estado (stateful inspection). Esta herramienta inserta un módulo denominado Inspection Module en el núcleo del sistema operativo sobre el que se instala, en el nivel software más bajo posible (por debajo incluso del nivel de res), así, desde ese nivel tan bajo, Firewall-1 puede interceptar y analizar todos los paquetes antes de que lleguen al resto del sistema; se garantiza que ningún paquete es procesado por ninguno de los

protocolos superiores hasta que Firewall-1 comprueba que no viola la política de seguridad definida. (www.checkpoint.com).

- **Pix:** Se trata de un firewall completamente hardware. PIX no se ejecuta en una máquina UNIX, sino que incluye un sistema operativo empotrado denominado Finesse que desde el espacio del usuario se asemeja más a un router que a un sistema Unix clásico. (www.cisco.com).
- **Zone alarm:** El firewall personal para Windows. Ofrecen una versión gratuita limitada. (www.zonelabs.com)

6.3.6 Detección de intrusos

Las herramientas de detección de intrusos permiten proteger a los sistemas mediante el uso de mecanismos que analizan actividades no lícitas.
Las más conocidas son las denominadas IDS (Intrusion Detection System). Una generación más actual son los Honeypots y Honeynets, que funcionan como señuelos.

6.3.6.1 Tipos de intrusos

Hay que aclarar que los intrusos son los individuos que llevan adelante los ataques y éstos pueden ser de dos tipos:

- **Externos:** Son personas no autorizadas a acceder en el sistema objeto de ataque.
- **Internos:** Son personas que tienen acceso a algunos recursos del sistema.

Los intrusos internos se clasifican en:

- **Enmascarados:** Son los que se ocultan tras la identidad de algún otro usuario legítimo con acceso a datos sensitivos. Los logs no logran detectar al verdadero atacante.

- **Clandestinos:** Son los que tienen acceso como para deshabilitar los controles de auditoría, para que no registren algunas actividades. Son los más peligrosos.

Para comprender mejor un ataque de intrusión interna se dará un ejemplo:

- "A" es un usuario legítimo con acceso al archivo de *sueldos* y "B" es un usuario también legítimo pero sin acceso al archivo *sueldos.*
- "B" compromete la contraseña de "A" (por cualquier método de los descritos anteriormente) y accede al sistema con la identidad de A y modifica el archivo *sueldos.*
- En los logs quedará registrado que "A" modificó el archivo *sueldos.*

Los más peligrosos son los sujetos que pueden deshabilitar los registros de auditoría. Su técnica consiste en:

a) Deshabilitar el registro en los logs;
b) Efectuar su acción intrusiva sin dejar registros;
c) Reactivar el registro en los logs.

Al descubrirse la intrusión no se encontrarán datos registrados que puedan ser de utilidad para investigar (origen, autor, entre otros).
Lo que sí es posible detectar es que los registros en los logs fueron deshabilitados por un cierto tiempo. En este caso se debe buscar al responsable entre los usuarios con accesos privilegiados.

6.3.6.2 Composición de los IDS (Sistemas de Detección de Intrusos)

Los IDS están compuestos por tres elementos básicos, los cuales son:

1. Fuente de Información: Proporciona los eventos del sistema. Estos eventos pueden ser:

- Logs o registros de auditoría, tanto del sistema operativo, como de las aplicaciones.

- Paquetes de red.

Estos no son excluyentes, ya que hay sistemas que los combinan para mejorar su capacidad de detección.

2. Motor de análisis: Busca evidencias de intrusiones y funciona de acuerdo con dos estrategias:

- **Detección de anomalías:** Consiste en comparar la actividad monitorizada con el uso normal del sistema.
- **Detección de mal uso:** Consiste en comparar la actividad monitorizada con el uso adecuado del sistema.

3. Mecanismo de respuesta: Actúa de acuerdo a los resultados del motor de análisis y ésta puede ser:

- **Pasiva:** El IDS emite una alarma al administrador señalando la situación detectada, pero no toma ninguna acción para detener la intrusión. Opera off-line. Analiza los logs y señala posibles intrusiones o violaciones para que el administrador tome las acciones apropiadas.
- **Activa:** Analiza los logs en tiempo real. Al detectar una posible intrusión, emite la alarma al administrador y además puede lanzar medidas inmediatas de protección en forma proactiva o reactiva.

Las medidas proactivas se toman después de que ocurrió el incidente de seguridad, con lo que se evita vuelva a suceder en el futuro. Ejemplo: Deshabilitar un servicio. Y las medidas reactivas se toman durante el momento del ataque, con lo que se evita que el mismo prospere.

Ejemplo: matar el proceso sospechoso, desconectar el usuario.

Ambos pueden ser tomados automáticamente por el propio IDS o manualmente por el administrador de seguridad ante la notificación del IDS.

6.3.6.3 Clasificación de los IDS

Los IDS se pueden clasificar en 2 tipos; según los sistemas que vigilen y según la estrategia que emplea su motor de análisis, mismos que se describen a continuación:

A. Según los sistemas que vigilen:

- **Basados en host (HIDS):** Examinan la actividad en un único equipo. Son muy simples de implementar y poco costosos, aunque su alcance es limitado, por ejemplo, si llegara a producirse una intrusión en otro host u otra parte de la red, este IDS no la detectará.
- **Basados en red (NIDS):** Monitorean todos los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella. Puede situarse en cualquiera de los *hosts* o en un servidor, en ambos casos su placa de red debe estar en modo promiscuo para capturar todo el tráfico y son capaces de detectar ataques provenientes del tráfico "ilícito" que dejó pasar el firewall.
- **Basados en agentes:** Están orientados a computación móvil y a sistemas distribuidos. Los agentes (programas autónomos pequeños) se ejecutan sobre el sistema que se desea proteger, monitoreando su actividad tal como en los HIDS, los datos recogidos por los agentes se envían a otras unidades del IDS donde se analizan en mayor profundidad. Algunos ejemplos de dichos sistemas son: AAFID (Autonomous Agents for Intrusion Detection) y EMERALD.

B. Según la estrategia que emplea su motor de análisis

- **Basados en detección de anomalías:** Parten de la siguiente consideración: ***"Todas las actividades de intrusión son actividades anómalas"*** Lo que significa que toda actividad anómala que detecte la va a considerar como una actividad intrusiva.

Por ello, para diferenciar los eventos anómalos de los eventos normales, el IDS se debe basar en el conocimiento previo de las actividades normales del sistema (perfil normal), así cómo, comparar cada evento contra el perfil normal. Un desvío significativo respecto a ese perfil normal será tomado como intento de intrusión.

Algunos ejemplos son:

- El usuario “mlopez” ingresa al sistema desde la estación de trabajo WSTD24 o desde WSTD25 en el horario de 8 a 16 hrs.
- La impresora LPTD190 emite listados de hasta 30 hojas.
- La estación de trabajo móvil WSM12 se conecta a la red diariamente entre las 20 y 21 hrs.

¿Pero qué pasa si?:

- El usuario “mlopez” debe trabajar un sábado a partir de las 18 hrs?
- Si se manda a imprimir a la impresora LPTD190 un documento de 50 páginas?
- Si la estación de trabajo móvil WSM12 se conecta a la red a las 23:30 hrs?

En todos esos casos el IDS detectará una intrusión.

O bien ¿Qué pasa si?:

- Otro empleado de la empresa aprovecha que “mlopez” salió a hacer un trámite y usa su estación de trabajo para mandar a imprimir por la impresora LPTD190 un documento confidencial de 23 páginas?.
- O si un objeto roba la estación de trabajo móvil WSM12 y se conecta normalmente?

En todos esos casos el IDS no detectará nada anormal. De estos ejemplos surge que: “el conjunto de actividades intrusivas no es exactamente igual al conjunto de actividades anómalas” Así como se muestra en la figura 6.10.

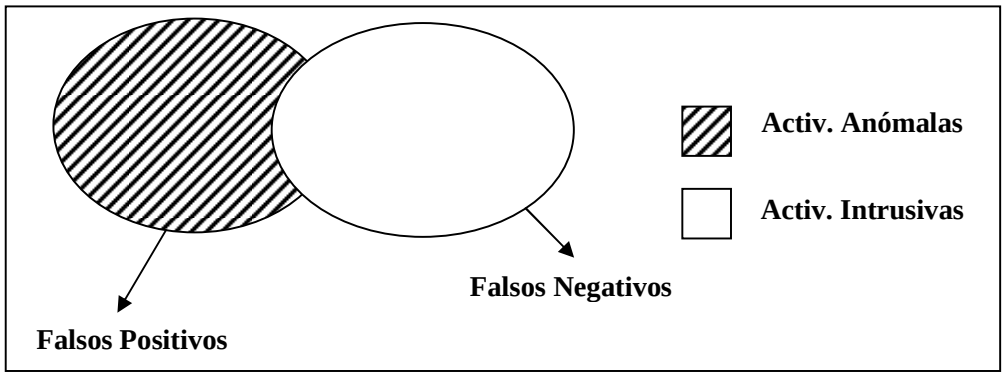


Figura 6.10 Ejemplo

Falsos Positivos: El IDS detecta actividades anómalas pero que no son intrusivas. Genera falsas alarmas, si el índice es alto, y puede resultar que el IDS sea ineficiente.

Falsos Negativos: El IDS desecha actividades intrusivas pero que no son anómalas. A mayor índice mayor riesgo tiene el sistema. Por lo tanto se puede decir, que los falsos negativos son mucho más peligrosos que los falsos positivos. El objetivo es minimizar ambos indicadores. Para ello es necesario seleccionar con cierto cuidado los aspecto del sistema que se van a monitorear y los umbrales de análisis, razón por la que es imprescindible que el administrador conozca la operatividad de la red.

- **Basados en mal uso:** Estos parten de la siguiente consideración: “Todas las actividades de intrusión se corresponden al uso incorrecto o mal uso del sistema o de algún recurso del mismo”.

Lo que significa que todo mal uso del sistema que detecte lo va a considerar como una actividad intrusiva.

Para este tipo de IDS el concepto de “mal uso” significa uso inadecuado y este uso inadecuado es el que sucede en el caso de las intrusiones o ataques. Por lo tanto para detectar “mal uso” los IDS se basan en los patrones de conducta o firmas. Por ello se deben comparar toda actividad en el sistema contra una base de datos de firmas de ataques:

- Dependiendo de su nivel de "inteligencia" son capaces de detectar variaciones de un mismo ataque aunque el mismo sea llevado a cabo con actividades diferentes.
- Pero, igual que los programas antivirus, no pueden hacer prácticamente nada en caso de un ataque desconocido, pues carecen de la firma que lo pueda identificar.
- La BD de firmas de ataques debe estar siempre actualizada.

Existen dos cuestiones importantes ligadas a la efectividad de este tipo de IDS:

- **Identificación de la firma asociada a un ataque:** No es fácil conocer todas las estrategias que emplean los atacantes para llevar a cabo un determinado ataque. A veces los ataques intercalan actividades correctas e inofensivas con las verdaderas actividades intrusivas, otras veces, realizan los ataques por etapas.
- **Distinción entre un ataque y una actividad no intrusiva:** Algunas actividades comunes tiene un patrón similar al de ciertos ataques: por ejemplo, un administrador escaneando la red mediante el comando *ping* se puede asemejar a la preparación de un ataque donde el intruso busca cuáles hosts están respondiendo.

C. Híbridos

Combinan aspectos de ambos tipos: detección de anomalías y detección de mal uso. Trabajan con una base de datos de firmas de ataques y también aprenden de ataques analizando el tráfico normal de la red. Si bien, poseen las ventajas de los dos modelos y son más eficientes y complejos de administrar.

Según la técnica que emplean los IDS se pueden clasificar en:

- **Basados en uso normal:** Se basan en comparaciones simples con los datos de registro generados por el sistema sin aplicar ningún tipo de "inteligencia", también, son los más comunes y los más simples de

implementar. Un dato interesante es que los primeros IDS utilizaban este modelo.

- **Basados en modelos estadísticos:** Este tipo de modelo incorpora algún grado de análisis a partir de los datos registrados en el sistema y establecen los posibles perfiles normales o uso adecuado mediante análisis estadísticos de los datos obtenidos de la fuente de información.
- **Basados en regla (predictivos):** Son más complejos ya que incorporan reglas a su motor de análisis para predecir posibles comportamientos anómalos o posibles usos indebidos. La mayor complejidad se basa en establecer las reglas.
- **Basados en razonamiento:** Una variante con respecto a los que se han mencionado anteriormente es que aplican técnicas de inteligencia artificial para razonar de acuerdo a reglas establecidas en un motor de inferencia, pudiendo llegar a detectar (y detener) ataques en progreso.
- La complejidad está dada no solo por las reglas sino por el motor de inferencia. Actualmente la mayoría de los IDS implementan este tipo de técnica.
- **Basados en transición de estados:** Se basan en analizar los estados resultantes como producto de las acciones realizadas, más que de analizar las secuencias de acciones en si mismas, de este modo pueden detectar ataques aunque se encuentres enmascarados en acciones legítimas.

Algunos productos de firewall’s son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **Prelude:** Es un IDS híbrido que trabaja junto con otras herramientas. (www.prelude-ids.org)
- **RealSecure:** Es un sistema de detección de intrusos y avisos automatizado en tiempo real, que detecta las actividades sospechosas y responde a los ataques a la red. (www.iss.com)

- **Snort**: Esta herramienta es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como MySQL. Esta herramienta implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.(www.snort.org)

Como se mencionó anteriormente, también están los Honeypots y los Honeynets, que funcionan como señuelos y se describen a continuación:

- **Honeypots**

Los Honeypots son sistemas señuelo que se usan para detectar y analizar intrusiones, así mismo, se implementan en una red para que puedan ser explorados y atacados mediante flujos de seguridad, preparados para atraer a los intrusos. Por esta razón pueden ser considerados cómo un tipo de IDS.
La idea de los Honeypots es que un atacante descubra un sistema “atacable” y efectúe su intrusión, comprometiendo los mecanismos de seguridad. El intruso cree que su ataque es efectivo sin darse cuenta de que en realidad fue realizado sobre un sistema aislado de la red.

Algunas de las características de los Honeypots son:

- Un honeypot no tiene utilidad desde el punto de vista de producción; por lo tanto, toda interacción con él es una intrusión o un intento de ésta.
- Es especialmente útil para estudiar las técnicas que emplean los intrusos y para aprender sobres nuevas técnicas de ataque.
- Esto permite reforzar el sistema verdadero y tomar medidas de seguridad anticipadas.

Existen dos tipos de *honeypots* de acuerdo al nivel de actividad que le permiten tener al atacante:

- **De baja interacción:** Operan únicamente emulando servicios y sistemas operativos, con lo que presentan al intruso una interacción restringida a lo que se esté emulando.
- **De alta interacción:** Operan en sistemas reales ofreciendo servicio y aplicaciones reales (no son emuladas), obviamente aislados de la red.

Ventajas:

- **Logs más pequeños:** Solo registran la actividad proveniente del exterior.
- **Nuevas herramientas y tácticas:** Permiten analizar herramientas o técnicas de ataque no vistas anteriormente.
- **Cifrado:** Operan bien en entornos cifrados como IPv6.

Desventajas:

- **Visión limitada:** Sólo pueden rastrear y capturar actividad que interactúen directamente con ellos.
- Los atacantes expertos y que verdaderamente tienen la intención de atacar pueden darse cuenta fácilmente de su existencia y pasarlo por alto.
- Tienen vulnerabilidades porque trabajan con las tecnologías existentes.

- **Honeynets**

Se define como un conjunto de Honeypots altamente interactivos, diseñados para la investigación y obtención de información sobre atacantes.
Un Honeynet es una arquitectura, no un producto de software determinado, su objetivo es hacerle creer al atacante que está ante una red “real”, entonces se deben añadir los distintos elementos que conforman una arquitectura de red.

La mayoría de los sistemas de seguridad han sido siempre de carácter defensivo, por ejemplo los IDS, firewalls y demás soluciones, se basan el a defensa de los sistemas de la organización y cuando un ataque o vulnerabilidad es detectado de inmediato se procede a corregirlo.

Con los Honeynets se obtienen nuevos patrones de comportamiento así como métodos de ataque cuyo objetivo es prevenirlos en los sistemas reales, sin éstos, cada vez que se produzca un ataque "nuevo" y exitoso a un sistema real existente, este dejará de dar servicio y se verá comprometido. Por el contrario con los Honeynets, un ataque exitoso o nuevo, no tiene porqué afectar a ningún sistema real.

6.3.7 Autenticación

Las redes y los servicios que prestan los servidores son cada vez más complejos. La red de una organización ya no se restringe a un único lugar físico, sino que puede estar distribuida en muchos ambientes geográficos con servidores ubicados en distintos lugares.

Frente a esta realidad es necesario garantizar que los servidores presten los servicios a clientes legítimos.
Las herramientas de autenticación surgen como una necesidad para garantizar la identidad de clientes ante servidores. La más común es Kerberos.

Kerberos fue creado en 1983 por el MIT para el proyecto Athena, éste tenía como objetivo crear un entorno de trabajo educacional compuesto por estaciones gráficas, redes de alta velocidad y servidores.
Un dato interesante es que en la mitología griega, kerberos es el nombre de un perro de tres cabezas que vigila la puerta de entrada al infierno.

Antes de kerberos, existían 2 modelos de autenticación:

1. Una vez que un usuario se autenticaba e ingresaba al sistema, podía usar todos los servicios que éste le ofrecía.
   El nivel de seguridad proporcionado era muy bajo, ya que el cliente adquiría demasiado poder sobre el servidor.

2. Cada vez que un cliente solicitaba un servicio, se debía volver a identificar y autenticar ante el servidor (por ejemplo, usar contraseñas para cada servicio de la red).

   Se obligaba al usuario a teclear su clave repetidamente; de tal forma que la contraseña viajaba muchas veces por la red, lo que hacía más probables los ataques exitosos.

Kerberos mejora estos esquemas porque exige que un cliente tenga autorización para comunicarse con un servidor y por que elimina la necesidad de demostrar el conocimiento de la contraseña.

Cuando un cliente solicita un servicio a un servidor, éste le exigirá al cliente un ticket de autorización antes de darle el servicio, este ticket, que es entregado por un servidor kerberos, a pedido del cliente, indicará que kerberos autorizó al cliente a pedirle un servicio al servidor.
Los ticket son entregados por kerberos después de que el cliente haya demostrado ser quien decía ser, si el cliente posee el ticket apropiado, el servidor supone que el cliente es legítimo.

Funcionamiento de Kerberos:

1. Un cliente inicia una sesión en la red.
2. Se autentica por única vez contra un servidor Kerberos.
3. Solicita servicios de un servidor “S”:
   i. Le pide a Kerberos un ticket que lo autentique ante el servidor “S”.
   ii. Luego se conecta al servidor “S”, le presenta el ticket y finalmente le solicita el servicio.

El paso número 3 será realizado cada vez que el cliente solicite un servicio. Un servidor Kerberos se denomina KDC (Key Distribution Center), y provee dos servicios fundamentales:

- **Autenticación (AS):** Autentica inicialmente al cliente proporcionándole un ticket especial (TGT – Ticket Grating Ticket), que posteriormente le servirá para demostrarle a Kerberos (más precisamente al Servicio de Concesión de Ticket) que ya fue autenticado.
- **Concesión de ticket (TGS):** Le proporciona al cliente los tickets que este debe presentar ante los servidores cuando solicite algún servicio.

Características principales de Kerberos:

- Se basa en la criptografía simétrica
- Requiere relojes sincronizados
- Debe conocer todas las claves privadas

El mecanismo de autenticación en Kerberos es un proceso que se realiza en tres grandes etapas (así cómo se muestra en la figura 6.11):

- **Login:** Procedimiento por el que un cliente se identifica y autentica ante un servidor Kerberos.
- **Obtención de ticket:** Procedimiento para solicitar al servidor Kerberos la provisión de tickets para acceder a los servidores.
- **Petición de servicios:** Solicitud de servicios a los servidores.

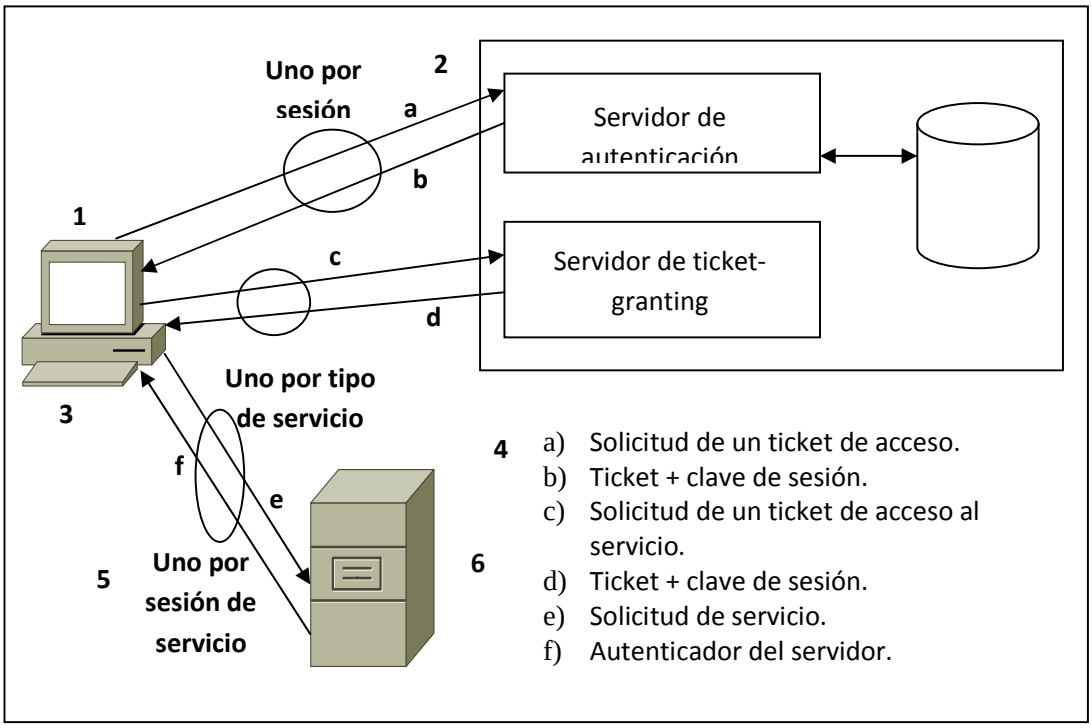


Figura 6.11 Mecanismo de autenticación en Kerberos

La arquitectura de Kerberos se basa en tres objetos de seguridad:

- **Clave de sesión:** Clave creada dinámicamente por kerberos durante una sesión para ser usada en la comunicación entre el cliente y un servidor.
- **Ticket:** Credencial que Kerberos le entrega a un cliente para que éste pueda demostrar que ha sido autenticado recientemente. Hay 2 clases de ticket: TGT (ticket para pedir ticket) y TS (ticket para pedir servicios).
- **Autenticador:** Elemento construido por el cliente con su nombre y la hora, cifrado con una clave de sesión entre el cliente y el TGS, que utiliza el TGS en verificar la identidad del cliente para poder extender los TS que éste solicita.

TGT: Es la credencial que el servicio de autenticación de Kerberos (AS) le entrega al cliente para que lo presente ante el servicio de concesión de ticket (TGS) cuando solicite credenciales para algún servicio.

TS: Es la credencial que el TGS le entrega al cliente para que lo presente ante el servidor al que le solicita servicios.

Cabe destacar que Kerberos es un sistema para garantizar la autenticidad, pero también proporciona integridad y confidencialidad.

Por ejemplo:

- Integridad: Cada paquete de datos se envía con un checksum cifrado con la clave de sesión.
- Confidencialidad: Cada paquete viaja cifrado con la clave de sesión.

Resulta que kerberos es el modelo más generalizado de aplicación del concepto *Single Sign On (SSO)* que consiste en que los clientes disponen de un único punto de identificación y autenticación en un entorno de red muy complejo, con muchos servicios distribuidos entre múltiples servidores.

Las principales desventajas son:

- Modelo centralizado.
- Necesidad de sincronización de los relojes de todas las máquinas que ejecuten servicios autenticados.
- Toda la red debe estar "Kerberizada".

Por lo tanto, se puede concluir que los Kerberos se encuentran disponibles para la mayoría de sistemas UNIX y es el sistema de autenticación elegido por Microsoft para Windows 2000, también incursiona en algunos conceptos avanzados de seguridad, tales como:

- Delegación
- Autenticación entre dominios
- Confianza transitiva
- Uso de claves públicas

Como se ha podido observar, existe una gran serie de herramientas que se pueden emplear para implantar el esquema de seguridad desarrollado, y aun cuando éstas no son todas ni las únicas que existen, sí son una amplia gama de posibilidades a estudiar y elegir aquellas que sean necesarias para el entorno (véase figura 6.12).

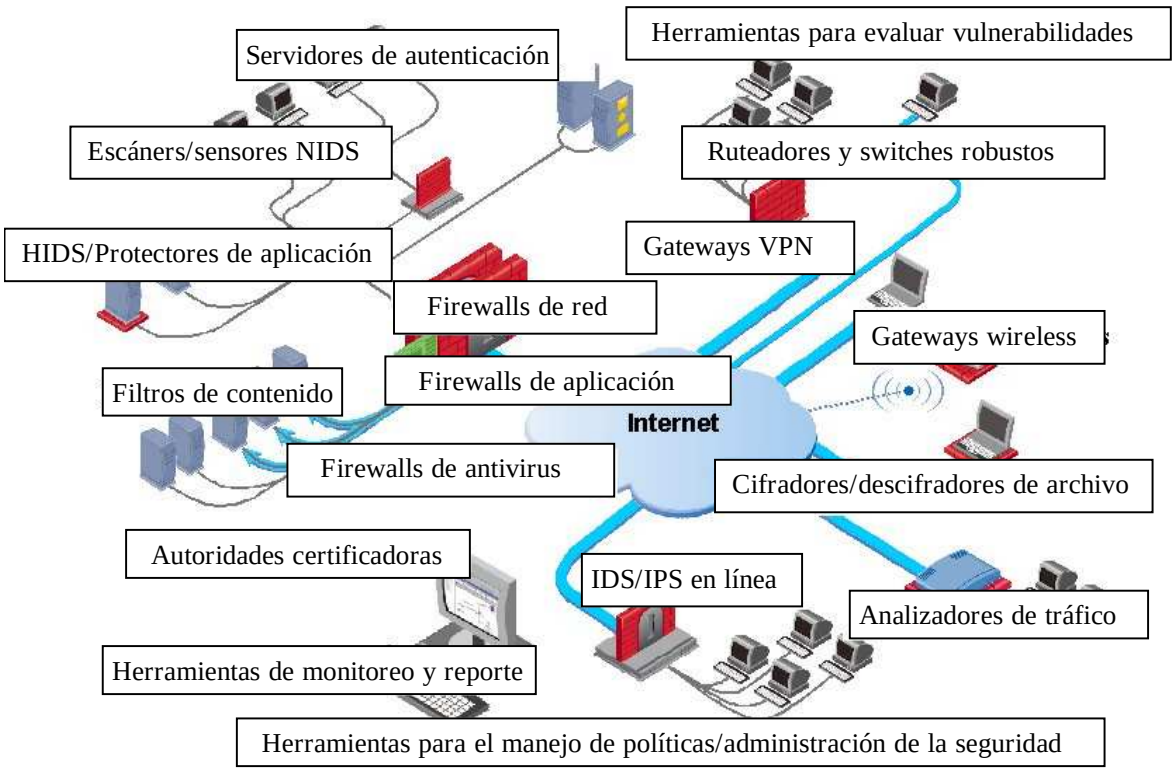


Figura 6.12 Uso de herramientas de seguridad

6.4 Auditoría

La auditoría resulta ser un tema de gran interés ya que con esta herramienta es posible identificar y corregir diversas vulnerabilidades existentes que suelen presentarse en las estaciones de trabajo, en las redes o en los servidores. Por ello es imprescindible conocer más a fondo los tipos de auditoría que existen así como las fases y los diversos estándares, los cuales se desarrollan a continuación.

La proliferación de metodologías en la auditoría y el control informático se observan en los primeros años de la década de los 80’s, paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas (como el software de análisis de riesgos).

6.4.1 Definición

Una auditoría de seguridad informática es el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables, quienes deberán establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas, aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

Algunos de los objetivos de la auditoría informática son:

- *El control de la función informática*
- *El análisis de la eficiencia de los Sistemas Informáticos*
- *La verificación del cumplimiento de la Normativa en este ámbito*
- *La revisión de la eficaz gestión de los recursos informáticos*

La auditoría informática sirve para mejorar las actividades informáticas en las empresas así como su eficiencia, eficacia, rentabilidad y seguridad.

Algunos de los objetivos específicos de la auditoría informática son:

- *El cumplimiento de controles de la transferencia de aplicaciones del entorno de desarrollo al entorno de explotación*
- *La concientización de la Dirección y de los usuarios en la seguridad de los SI*
- *El cumplimiento de la legislación vigente*
- *La remuneración de los recursos humanos del departamento de SI*

- *Los procedimientos del Centro de Información*

6.4.2 Auditoría interna y auditoría externa

La Auditoría interna es realizada por una entidad funcional perteneciente a la propia estructura organizativa de la empresa y como contraprestación reciben una remuneración económica. La principal ventaja de la auditoría interna es que quienes son los responsables de llevarla a cabo pertenecen a la propia empresa, y que, por tanto, conocen directamente su problemática. Por otra parte el costo será menor puesto que los recursos utilizados emanan de la propia organización.

Por otro lado la Auditoría externa se realiza por personas ajenas a la empresa. La empresa contrata un servicio profesional para auditar su sistema de información por expertos externos a la empresa. La principal ventaja es el alto grado de objetividad que se consigue en comparación con la anterior. El principal inconveniente viene dado por el alejamiento de la problemática de la empresa de quienes asumen la responsabilidad de llevar a cabo la auditoría. No obstante, la profesionalidad y la experiencia de quienes asumen la auditoría debe superar estos inconvenientes para llevar a cabo un trabajo profesional. La auditoría externa desde el punto de vista económico es más costosa que la interna.

6.4.3 Características de la Auditoría informática

La Auditoría informática no suele realizarse de forma periódica en las organizaciones, sino que surge como consecuencia de problemas reales o potenciales, excepto cuando alguna normativa legal obliga, periódicamente o no, a su realización.
Agrupando por áreas esos problemas, las causas que pueden originar la realización de una Auditoría Informática son:

- **Desorganización / Descoordinación**
    - No coincidencia de objetivos del sistema de Información (SI) con los objetivos de la Organización

  - Los circuitos de información no son los adecuados
  - Duplicidad de información
  - No disponibilidad de la información o de resto de los recursos de la SI
- **Insatisfacción de usuarios**
  - No resolución de incidencias y averías
  - No atención de peticiones de cambios
  - Inadecuado soporte informático
  - Incumplimiento en los plazos de entrega de resultados periódicos
- **Debilidades económico – financieras**
  - Incremento inadecuado de las inversiones
  - Aumento constante de los costos
  - Desviaciones presupuestarias significativas
  - Incremento de recursos en el desarrollo de proyectos
- **Inseguridad de los SI**
  - Escasa confidencialidad de la información
  - Falta de protección física y lógica
  - Inexistencia de planteamientos en cuanto a la continuidad del servicio
- **Cumplimiento de la legalidad**
  - Protección de datos de carácter personal
  - Cumplimiento en TI por la ley Sarbanes - Oxley[48]

6.4.4 Tipos y clases de auditorías

El departamento de informática posee una actividad proyectada al exterior, al usuario, aunque el "exterior" siga siendo la misma empresa, por lo tanto, de ahí surge la *Auditoría Informática de Usuario.* Ésta se distingue para contraponerla a la Informática

[48] La ley Sarbanes Oxley nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en bolsa, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor.
http://forodeseguridad.com/artic/segcorp/7217.htm

Interna, en donde se hace la informática cotidiana y real. En consecuencia, existe una *Auditoría de Actividades Internas.*

Por otra parte, el control del funcionamiento del departamento de informática referente al exterior, con el usuario se realiza por medio de la Dirección, ya que ésta es capaz de interpretar las necesidades de la Compañía. Por ello, una informática eficiente y eficaz requiere el apoyo continuo de su Dirección frente al "exterior". Revisar estas interrelaciones constituye el objeto de la *Auditoría Informática de Dirección.* Estas tres auditorías, más la auditoría de Seguridad, son las cuatro Áreas Generales de la Auditoría Informática más importantes, dentro de éstas se establecen las siguientes divisiones de auditoría informática: Explotación, Desarrollo de Proyectos, Sistemas, Comunicaciones y Seguridad, las cuales se muestran en la tabla 6.1

Tabla 6.1 Divisiones de Auditoría Informática

Áreas Específicas	Áreas Generales			
	Interna	Dirección	Usuario	Seguridad
Explotación				
Desarrollo de Proyectos				
Sistemas				
Comunicaciones				
Seguridad				

Cada área específica puede ser auditada desde los siguientes criterios generales:

- Su propio funcionamiento interno
- El apoyo que recibe la dirección y en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- La perspectiva de los usuarios, destinatarios reales de la informática.
- El punto de vista de la seguridad que ofrece la informática en general o la rama auditada.

Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

6.4.5 Fases de una auditoría

Los servicios de auditoría constan de las siguientes fases:

Fase I: Conocimientos del sistema

- *Aspectos Legales y Políticas Internas:* Sobre estos elementos está construido el sistema de control y por lo tanto constituyen el marco de referencia para su evaluación.
- *Características del Sistema Operativo.*
    - Organigrama del área que participa en el sistema.
    - Manual de Funciones de las personas que participan en los procesos del sistema.
    - Informes de auditorías realizadas anteriormente.
- *Características de la aplicación de computadora.*
    - Manual técnico de la aplicación del sistema.
    - Funcionarios (usuarios) autorizados para administrar la aplicación.
    - Equipos utilizados en la aplicación de computadora.
    - Seguridad de la aplicación (claves de acceso).
    - Procedimientos para generación y almacenamiento de los archivos de la aplicación.

Fase II: Análisis de transacciones y recursos

- *Definición de las transacciones:* Dependiendo del tamaño del sistema, las transacciones se dividen en procesos y estos en subprocesos. La importancia de las transacciones deberá ser asignada con los administradores.
- *Análisis de las transacciones.*
    - Establecer el flujo de los documentos.

    En esta etapa se hace uso de los flujogramas (representación gráfica de la secuencia de actividades de un proceso[49]) ya que facilita la visualización del funcionamiento y recorrido de los procesos.
- *Análisis de los recursos:* Consiste en identificar y codificar los recursos que participan en los sistemas.

[49] http://www.infomipyme.com/Docs/GENERAL/Offline/GDE_04.htm

- *Relación entre transacciones y recursos.*

Fase III: Análisis de riesgos y amenazas

- La *Identificación de riesgos* consiste en identificar los siguientes aspectos:
    - Daños físicos o destrucción de los recursos
    - Pérdida por fraude o desfalco
    - Extravío de documentos fuente, archivos o informes
    - Robo de dispositivos o medios de almacenamiento
    - Interrupción de las operaciones del negocio
    - Pérdida de integridad de los datos
    - Ineficiencia de operaciones
    - Errores
- *Identificación de las amenazas.*
    - Amenazas sobre los equipos
    - Amenazas sobre documentos fuente
    - Amenazas sobre programas de aplicaciones
- *Relación entre recursos, amenazas y riesgos.*

La relación entre estos elementos deberá establecerse a partir de la observación de los recursos en su ambiente real de funcionamiento.

Fase IV: Análisis de controles

- *Codificación de controles.*

Los controles se aplican a los diferentes grupos utilizadores de recursos, donde la identificación de los controles debe contener una codificación la cual identifique el grupo al que pertenece el recurso protegido.

- *Relación entre recursos, amenazas y riesgos.*

La relación con los controles debe establecerse para cada tema (recursos, amenazas y riesgos) identificado. Para cada tema debe establecerse uno o más controles.

- *Análisis de cobertura de los controles requeridos.*

Este análisis tiene como propósito determinar si los controles que el auditor identificó como necesarios proveen una protección adecuada de los recursos.

Fase V: Evaluación de controles

- *Objetivos de la evaluación.*

Consiste en:

  - Verificar la existencia de los controles requeridos.
  - Determinar la operatividad y suficiencia de los controles existentes.

- *Plan de pruebas de los controles.*
  - Incluye la selección del tipo de prueba a realizar.
  - Deben solicitarse al área respectiva todos los elementos necesarios de prueba.
- *Pruebas de controles.*
- *Análisis de resultados de las pruebas.*

Fase VI: Informe de auditoría

- *Informe detallado de recomendaciones.*
- *Evaluación de las respuestas.*
- *Informe resumen para la alta gerencia.*

Este informe debe prepararse una vez obtenidas y analizadas las respuestas de compromiso de las áreas y debe contemplar los siguientes aspectos:

- **Introducción:** Objetivo y contenido del informe de auditoría.
- **Objetivos** de la auditoría.
- **Alcance:** cobertura de la evaluación realizada.
- **Opinión:** con relación a la suficiencia del control interno del sistema evaluado.
- **Hallazgos**
- **Recomendaciones**

Fase VII: Seguimiento de las Recomendaciones.

- *Informes del seguimiento.*
- *Evaluación de los controles implantados.*

6.4.6 Auditoría de seguridad de la información

La auditoría de seguridad de la información tiene por objetivo verificar que se cumplan los controles estipulados por la organización. Esto puede hacerse bien en un "documento de seguridad", a través de unas Políticas de Seguridad, en un Plan de Seguridad o mediante unos Objetivos de Control de carácter sectorial o general.

Existen diferentes tipos de auditoría de seguridad, los cuales son:

- **Auditoría de seguridad física:** Se refiere a la ubicación de la organización, evitando ubicaciones de riesgo y en algunos casos no revelando la situación física de ésta. También se refiere a las protecciones externas (vigilantes, arcos de seguridad, entre otros) y protecciones del entorno.
- **Auditoría de seguridad lógica:** Comprende los métodos de autenticación de los sistemas de información.
- **Auditoría de seguridad en el desarrollo de las aplicaciones:** comprende la revisión de las metodologías utilizadas y el control interno de las aplicaciones. En la primera se analizan las metodologías, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la aplicación y el fácil mantenimiento de las mismas. En la segunda se revisan las fases que se deben seguir acorde al área de desarrollo, por ejemplo:
  - **Estudio de viabilidad de la aplicación:** para aplicaciones largas, complejas y caras.
  - **Definición lógica de la aplicación:** Se analizan las posturas lógicas de actuación, en función de la metodología elegida y la finalidad que persigue el proyecto.
  - **Desarrollo técnico de la aplicación:** Se verifica que éste sea ordenado y correcto.
  - **Diseño de programas:** Deberán poseer la máxima sencillez, modularidad y economía de recursos.
  - **Métodos de pruebas: Se** realizan de acuerdo a las normas de instalación.
  - **Documentación:** Debe cumplir con la norma establecida en la instalación, tanto en la de Desarrollo como en la de Aplicaciones a Explotación.

- **Equipo de programación:** Se deben fijar las tareas de análisis puro, de programación y las intermedias.

- **Auditoría de seguridad en el área de producción:** Se refiere a los errores que pueden ocurrir así mismo cómo accidentes y fraudes.
- **Auditoría de seguridad en los datos:** Se refiere a la clasificación de los datos, estudio de las aplicaciones y análisis de los diagramas de flujo.
- **Auditoría de las bases de datos:** Se refiere a los controles de acceso, de actualización
- **Auditoría de seguridad en comunicaciones y redes:** Hace referencia a la auditoría de los procesos de autenticación en los sistemas de comunicación.
- **Auditoría de la gestión:** Referido a la contratación de bienes y servicios, documentación de los programas, entre otros.
- **Auditoría legal del reglamento de protección de datos:** Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento desarrollo de la "Ley Orgánica de Protección de Datos"

Como áreas sobre las que ha de actuar la auditoría informática se pueden considerar las siguientes:

a) **Fundamentos de la seguridad:** Políticas, planes, funciones, existencia y funcionamiento de algún comité relacionado, objetivos de control, presupuesto, así como que existen sistemas y métodos de evaluación periódica de riesgos.
b) **Desarrollo de las políticas:** Procedimientos, posibles estándares, normas y guías.
c) **Amenazas físicas externas:** Inundaciones, incendios explosiones, cortes de líneas de comunicaciones, terremotos, terrorismo y huelgas.
d) **Control de accesos adecuado tanto físicos como lógicos:** De manera que cada usuario pueda acceder a los recursos para los que esté autorizado y asimismo pueda realizar solo las funciones permitidas.

e) **Protección de datos:** Según lo que regula la ley orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal y el reglamento 994/1999
f) **Comunicaciones y redes:** Topología y tipo de comunicaciones, uso de cifrado y protecciones ante virus.
g) **Entorno de Producción:** Entendiendo como tal la explotación más Técnica de Sistemas.
h) **Desarrollo de aplicaciones en un entorno seguro.**
i) **Continuidad de las operaciones.**

6.4.7 Enfoques de la Auditoría Informática

Los enfoques asignados a la Auditoría informática son: Auditoría alrededor de, a través de, y auditoría con la computadora.

Auditoría alrededor de la computadora: En este enfoque de auditoría, los programas y los archivos de datos no se auditan.
La auditoría alrededor de la computadora enfoca sus esfuerzos en la entrada de datos y en la salida de la información. Es el más cómodo para los auditores de sistemas, por cuanto únicamente se verifica la efectividad del sistema de control interno en el ambiente externo de la máquina. También se examinan los controles desde el origen de los datos para protegerlos de cualquier tipo de riesgo que atente contra la integridad, exactitud y legalidad.

Los objetivos de este tipo de auditoría son:

- Verificar la existencia de una adecuada segregación funcional.
- Comprobar la eficiencia de los controles sobre seguridades físicas y lógicas de los datos.
- Asegurarse de la existencia de controles dirigidos a que todos los datos enviados a proceso estén autorizados.

- Comprobar la existencia de controles para asegurar que todos los datos enviados sean procesados.
- Cerciorarse que los procesos se hacen con exactitud.
- Comprobar que los datos sean sometidos a validación antes de ordenar su proceso.
- Verificar la validez del procedimiento utilizado para corregir inconsistencias y la posterior realimentación de los datos corregidos al proceso.
- Examinar los controles de salida de la información para asegurar que se eviten los riesgos entre sistemas y el usuario.
- Verificar la satisfacción del usuario. En materia de los informes recibidos.
- Comprobar la existencia y efectividad de un plan de contingencias, para asegurar la continuidad de los procesos y la recuperación de los datos en caso de desastres.

Auditoría a través de la computadora: Este enfoque está orientado a examinar y evaluar los recursos del software y surge como complemento del enfoque de auditoría alrededor de la computadora, en el sentido de que su acción va dirigida a evaluar el sistema de controles diseñados para minimizar los fraudes y los errores que normalmente tienen origen en los programas.

Los objetivos de esta auditoría son:

- Asegurar que los programas procesan los datos, de acuerdo con las necesidades del usuario o dentro de los parámetros de precisión previstos.
- Cerciorarse de la no-existencia de rutinas fraudulentas al interior de los programas.
- Verificar que los programadores modifiquen los programas solamente en los aspectos autorizados.
- Comprobar que los programas utilizados en producción son los debidamente autorizados por el administrador.

- Verificar la existencia de los controles eficientes para evitar que los programas sean modificados con fines ilícitos o que se utilicen programas no autorizados para los procesos corrientes.
- Cerciorarse que todos los datos sean sometidos a validación antes de ordenar su proceso correspondiente.

Auditoría con la computadora: Este enfoque va dirigido especialmente, al examen y evaluación de los archivos de datos en dispositivos de almacenamiento, con la ayuda de la computadora y de software de auditoría generalizados a la medida.

Los paquetes de auditoría permiten desarrollar operaciones y prueba, tales como:

- Recálculos y verificación de información, como por ejemplo, relaciones sobre nómina, montos de depreciación y acumulación de intereses, entre otros.
- Demostración gráfica de datos seleccionados.
- Selección de muestras estadísticas.
- Preparación de análisis de cartera por antigüedad.

Estos tres enfoques de auditoría mencionados son complementarios así como se muestran en la figura 6.13. Ninguno de los tres es suficiente para auditar aplicaciones en funcionamiento.

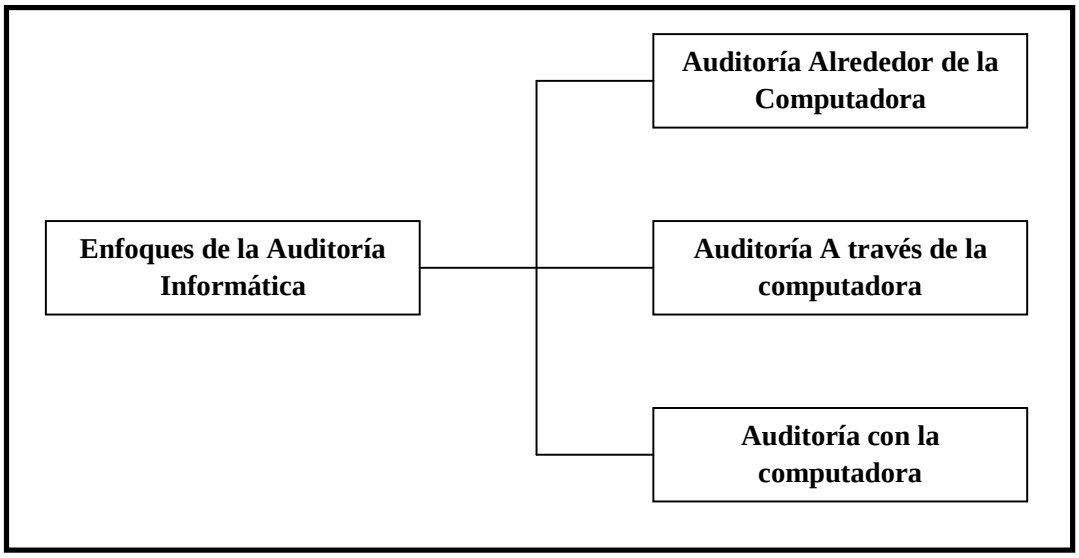


Figura 6.13 Enfoques de la auditoría informática.

6.4.8 Herramientas y técnicas para la auditoría informática

Cuestionarios

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos.

Para esto, suele ser habitual que se comience por solicitar el cumplimiento de cuestionarios preimpresos, que se envían a las personas que el auditor considera que son las adecuadas.

Estos cuestionarios no deben ser repetidos, sino que deben ser específicos para cada situación.

Entrevistas

El auditor comienza a realizar entrevistas con el personal de la empresa y lo hace de tres maneras:

1. Mediante la petición de documentación sobre alguna materia de su responsabilidad.
2. Mediante “entrevistas” en las que no se sigue un plan determinado ni un método estricto de sometimiento a un cuestionario.
3. Por medio de entrevistas en las que el auditor sigue un método preestablecido y busca finalidades concretas.

La entrevista entre el auditor y el auditado se basa en el concepto de interrogatorio y el auditor sigue en forma cuidadosa un sistema previamente establecido haciendo que la conversación sea lo menos tensa posible para que el auditado conteste de manera clara y sencilla.

Checklist

En esta etapa el auditor reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber y por qué. Sus cuestionarios son espacios vitales para el trabajo de análisis.

Ejemplo de un checklist:

Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y dentro de ella, se analiza el control de los accesos de personas y cosas al centro de cálculo. Podrían formularse las siguientes preguntas:

- ¿Existe personal específico de vigilancia externa al edificio?
  Re: No, solamente un guardia por la noche que atiende además otra instalación adecente.

<Puntuación: 1>

- Para la vigilancia interna del edificio, ¿hay al menos un vigilante por turno en los aledaños del Centro de Cálculo?
  Re: Si, pero sube a las otras 4 plantas cuando lo necesita.
  <Puntuación: 2>
- ¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?
  Re: Si, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan.
  <Puntuación: 2>

Así como estas preguntas, existen otras qué dependiendo de lo que se esté auditando, es cómo se resuelven los cuestionarios que realiza el auditor.

6.4.9 Perfil Profesional del auditor informático

A continuación en la tabla 6.2 se muestran algunas ocupaciones con sus respectivos perfiles que se deben cubrir para ser un auditor informático.

Tabla 6.2 Perfil Profesional del auditor informático

Ocupación	Actividades y conocimientos deseables
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el marcado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas	Con experiencia en el mantenimiento de bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación.
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Experto en Subsistemas de teleproceso.
Técnico de Organización.	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costos	Economista con conocimiento de informática. Gestión de costos.

De lo anteriormente mencionado se puede decir que para ser un auditor en materia de seguridad informática se requiere tener conocimientos especializados en las diversas ramas que existen. Por ello es de suma importancia que los futuros profesionistas, tengan la preparación adecuada, de tal manera que les sea posible cubrir las necesidades que las organizaciones demandan.

Se puede concluir que la auditoría informática juega un papel muy importante en las organizaciones, ya que se debe garantizar en la medida de lo posible, que la información que éstas manejan, sea íntegra, confiable y sobre todo que se encuentre disponible cuando ésta se requiera. Por ello, se tienen que realizar auditorías de manera

periódica, para asegurarse de que las normas que se establecieron al diseñar los sistemas de seguridad, cumplan y mantengan las normas establecidas.

6.5 Seguridad en redes inalámbricas

En los últimos años las redes inalámbricas han tomado un papel muy importante y día con día son más los usuarios que disponen de éstas. Hoy en día la mayoría de las personas que disponen de una computadora o laptop se conectan por medio de su tarjeta inalámbrica en diversos puntos de acceso, como lo son; las escuelas, bibliotecas, restaurantes, cafés, espacios públicos, entre otros.

El auge de las redes inalámbricas ha surgido debido a la facilidad que hay para conectarse a Internet, por ejemplo, ahora ya no se requieren de cables para conectarse a esta red, debido a que son fáciles de instalar, son flexibles, es decir, es posible instalar nuevas WLAN o cambiarlas, y también tienen la característica de ser escalables (se puede realizar una instalación empezando por pequeñas “redes ad-hoc” de unas pocas estaciones, e ir ampliándolas hasta hacerlas muy grandes por medio de la utilización de puentes inalámbricos).
Por ello se vuelve importante mantener un nivel de seguridad que permita que la información viaje de manera segura logrando cumplir con los principios básicos de la seguridad; integridad, confiabilidad y disponibilidad.

6.5.1 Definición de la seguridad inalámbrica

La palabra seguridad abarca un amplio rango de campos dentro y fuera del ámbito de la computación. Se habla de seguridad cuando se describe por ejemplo una nueva plataforma de cómputo y que se dice que ésta es segura. Por ello se puede decir que el término “seguridad inalámbrica” se encuentra dentro del contexto de la seguridad de la información, es decir, cuando se hace referencia a la seguridad inalámbrica se está

hablando de la seguridad de la información que se mueve a través de las redes inalámbricas.

Para entender el significado de la seguridad informática es necesario entender la manera en que el término ha evolucionado a lo largo del tiempo. Hasta finales de los años 70's, esta área de seguridad fue referida como "Seguridad de Comunicaciones" o COMSEC, por un acrónimo en inglés definido por la U.S. National Security Telecomunications and Information Systems Security Instruction (NSTISSI) como: "Medidas y controles que se toman para negar el acceso no autorizado de personas a información derivada de las telecomunicaciones y augurar la autenticidad de tales telecomunicaciones".

Se incluyeron cuatro áreas como partes de las actividades de seguridad COMSEC y son:

1. Criptoseguridad.
2. Seguridad de transmisiones.
3. Seguridad de emisiones.
4. Seguridad física.

La seguridad en COSMEC incluyó dos atributos los cuales son: *Confidencialidad y Autenticación.*

La *confidencialidad* consiste en asegurar que la información no sea divulgada a personas, procesos o dispositivos no autorizados.
La *Autenticación* es la medida de seguridad diseñada para establecer la validez de una transmisión, mensaje o remitente, o un medio para verificar la autorización de un individuo para recibir categorías específicas de información (verificación de emisor).

En los 80's con el crecimiento de las computadoras personales se inició una nueva era: Computación personal y la seguridad aplicada a este campo (COMPUSEC), ésta fue definida por NSTISSI como: *"Medidas y controles que aseguran la confidencialidad,*

integridad y disponibilidad de sistemas de información incluyendo hardware, software, firmware e información que está siendo procesada, almacenada y comunicada".
COMPUSEC introdujo dos atributos de seguridad adicionales, los cuales son: *Integridad y Disponibilidad.*

La *Integridad* es la calidad de un sistema de información que refleja el correcto funcionamiento y confiabilidad del sistema operativo, la coherencia del hardware y software que implementan los sistemas de protección y la consistencia de las estructuras de datos de la información almacenada.

La *Disponibilidad* se refiere al acceso oportuno y confiable a datos y servicios de información para usuarios autorizados.
Finalmente en los 90's, las dos eras de la información, COMSEC y COMPUSEC, fueron integradas para formar Seguridad en Sistemas de Información (INFOSEC); ésta incluyó los cuatro atributos: Confidencialidad, Autenticación, Integridad y Disponibilidad, pero también se agregó un nuevo atributo: No repudio (non repudiation).

El *No repudio (rendición de cuentas)* consiste en asegurar que el remitente de la información es provisto de una prueba de envío y que el receptor es provisto de una prueba de la identidad del remitente, de manera que ninguna de las partes puede negar el proceso de dicha información.

Seguridad de la información y las WLAN

La NSTISSI define el concepto de Seguridad de Sistemas de información como *"la protección de los sistemas de información contra el acceso no autorizado o la modificación de la información, ya sea en el medio de almacenaje, procesamiento o tránsito y contra la negación de servicio a los usuarios autorizados, o la provisión de servicio a usuarios no autorizados incluyendo las medidas necesarias para detectar, documentar y contabilizar esas amenazas"*.

Por ello, la seguridad inalámbrica se presenta desde el punto de vista de la "seguridad de los sistemas de información" o INFOSEC.

6.5.2 Implementación de los atributos de seguridad

El modelo de referencia OSI (Interconexión abierta de sistemas), creado por la ISO (organización internacional de estándares), es una descripción abstracta para el diseño de protocolos de redes de computadoras. El modelo divide las diferentes funciones de comunicación en siete capas que pueden funcionar de manera independiente una de otra.

Los estándares de redes inalámbricas se refieren normalmente a las capas 1 y 2 de la pila de protocolos OSI, conservando el paquete IP sin cambios. Los paquetes IP transportan sobre protocolos del nivel físico y de enlace de datos que son específicamente de carácter inalámbricos. Por ejemplo si se considera la "confidencialidad del tráfico de datos" entre dos puntos de acceso, se pueden lograr resultados similares (protección de la información) actuando en tres capas diferentes:

1. La capa de aplicación (mediante Transport Layer Security/Secure Sockets Layer).
2. La capa IP (mediante IPSEC).
3. La capa de enlace (mediante cifrado).

Hay que recordar que cuando se habla de seguridad inalámbrica, sólo se están examinando los mecanismos de seguridad concernientes a las capas 1 y 2, es decir, del cifrado nivel de enlace. Otros mecanismos de seguridad presentes a nivel 3 y superiores son parte de la seguridad implementada en las capas de red o de aplicación.

- **Cifrado a nivel de enlace**: El cifrado en el nivel de enlace es el proceso de asegurar los datos cuando son transmitidos entre dos nodos sobre el mismo enlace físico (puede ser también el caso de dos enlaces diferentes mediante un repetidor, ejemplo

un satélite). Con cifrado a nivel de enlace, cualquier otro protocolo o aplicación de datos que se ejecuta sobre el enlace físico queda protegida de cualquier intercepción.

El cifrado requiere una clave secreta compartida entre las partes en contacto y un algoritmo previamente acordado. Cuando el transmisor y receptor no comparten un medio de transporte de datos en común, los datos deben ser descifrados y nuevamente cifrados en cada uno de los nodos en el camino al receptor.
El cifrado en el nivel de enlace se usa en caso de que no se aplique un protocolo de mayor nivel.

- **Cifrado a nivel de enlace en el estándar IEEE 802.11:** El algoritmo de cifrado mejor conocido para el estándar IEEE 802.11 es el llamado en inglés Wired Equivalent Privacy (WEP). Está Probado que WEP es inseguro, y otras alternativas, como el protocolo WiFi Protected Acces (WPA), es considerado como el estándar recomendado. El nuevo estándar IEEE 802.11i incluye una extensión de WPA, llamada WPA2.

El cifrado a nivel de enlace no provee **seguridad de extremo a extremo,** fuera del enlace físico y sólo debe ser considerada una medida adicional en el diseño de la red. Este cifrado requiere más recursos de hardware en los puntos de acceso y medidas especiales de seguridad en la administración y distribución de claves.

6.5.3 Servicios de seguridad en redes inalámbricas

6.5.3.1 Confidencialidad

La confidencialidad en las redes inalámbricas es de suma importancia debido a que los datos que viajan en un medio poco seguro o no seguro requiere de mecanismos que garanticen de manera satisfactoria la transmisión de datos, por ello existen protocolos de seguridad diseñados para este tipo de transmisión los cuales son WEP, WPA y WPA2.

- **WEP o no WEP:** Se define la confidencialidad en redes inalámbricas como el acto de asegurar que la información transmitida entre los puntos de acceso y los clientes no sea revelada a personas no autorizadas. La confidencialidad debe asegurar que, ya sea la comunicación entre un grupo de puntos de acceso en un sistema de distribución inalámbrico (WDS por sus siglas en inglés), o bien entre un punto de acceso (AP) y una estación o cliente, se conserva protegida contra intercepciones.

  La confidencialidad en redes inalámbricas ha sido asociada tradicionalmente con el término "privacidad equivalente a enlaces alambrados" o WEP, el cual fue parte del estándar IEEE 802.11 original, de 1999.

  El propósito del WEP fue brindar, a las redes inalámbricas, un nivel de seguridad comparable al de las redes alambradas tradicionales. La necesidad de un protocolo como WEP fue obvio, las redes inalámbricas usan ondas de radio y son más susceptibles de ser interceptadas.

  La vida del WEP fue muy corta, debido a un mal diseño y por ser poco transparente condujo a ataques muy efectivos o a su implantación y tan sólo unos meses de que el WEP fuera publicado, el protocolo fue considerado obsoleto. Aunque la llave que tenía era de longitud limitada por las restricciones de exportación, se pudo comprobar que el protocolo era débil independientemente de ese hecho.
  No fueron sólo las fallas de diseño las que hicieron que WEP fuera obsoleto, sino también la falta de un sistema de manejo de claves como parte del protocolo, de manera que WEP no tuvo incluido sistema alguno de manejo de claves, así que, el sistema de distribución de claves fue tan simple como teclear manualmente la misma clave en cada dispositivo de la red inalámbrica.

WEP fue seguido por varias extensiones de carácter propietario que resultaron también inadecuadas, por ejemplo WEP+ de Lucent, y WEP2 de Cisco.

WEP y sus extensiones (WEP+, WEP2) son al día de hoy obsoletas. WEP está basado en el algoritmo de cifrado RC4, cuyas implementaciones en el estándar IEEE 802.11 se consideran inadecuadas debido a que es un protocolo vulnerable contra ataques a sus mecanismos de seguridad violando la privacidad, autenticidad e integridad de la información.

Existen varios ataques y programas para hacer sucumbir el WEP (Airsnort, wepcrack, kismac, y aircrack entre otros). Algunos de los ataques están basados en la limitación numérica de los vectores de inicialización del algoritmo de cifrado RC4, o la presencia de la llamada "debilidad IV" en un datagrama.

- **WPA y WPA2:** Luego del deceso del WEP, en 2003 se propone el Acceso Protegido a Wi-Fi (WPA, por sus iniciales en inglés) quedando certificado como parte del estándar IEEE 802.11i, con el nombre de WPA2 (en el 2004) WPA y WPA2 son protocolos diseñados para trabajar con y sin un servidor de manejo de claves. Si no se usa un servidor de claves, todas las estaciones de la red utilizan una "llave previamente compartida" (PSK – Pre-Shared-Key). El modo PSK se conoce como WPA o WPA2 – Personal.

  Por otra parte, mientras se emplea un servidor de claves, al WPA2 se le conoce como WAP2 – Corporativo (o WPA2 - Enterprise). En el WPA2 se usa un servidor IEEE 802.1x para distribuir las claves.

  Una mejora notable en el WPA sobre el antiguo WEP es la posibilidad de intercambiar claves de manera dinámica mediante un protocolo de integridad temporal de claves (TKIP – Temporal Key Integrity Protocol).

- **WPA2 – Acceso protegido a Wi-Fi:** WPA2 es la versión certificada de WPA y es parte del estándar IEEE 802.11i.

  Hay dos cambios principales en WPA2 y WPA, los cuales son:

  1. El reemplazo del algoritmo Michael por un código de autenticación conocido como el protocolo "Counter-Mode/CBC-Mac" (CCMP), que es considerado criptográficamente seguro.
  2. El reemplazo del algoritmo RC4 por el "Advanced Encryption Estándar (AES)" conocido también como Rijndael.

Se recomienda para la confidencialidad de datos que:

- Si se necesita confidencialidad mediante el cifrado a nivel de enlace, la mejor opción es WPA2 en modo corporativo (WPA2-Entreprise)
- En caso de usarse una solución más simple como la WPA2-Personal, deben tomarse precauciones especiales al escoger una contraseña (clave pre-compartida, PSK).

  Por lo tanto, el protocolo WEP y sus variantes WEP+ y WEP2, deben ser descartados.

6.5.3.2 Autenticación

En el caso de las redes LAN, la autenticación es la medida diseñada para establecer la validez de una transmisión entre puntos de acceso y/o estaciones inalámbricas. En otros términos, la autenticación inalámbrica significa "el derecho a enviar hacia y mediante el punto de acceso".

Para entender la "Autenticación" en redes inalámbricas es necesario entender qué sucede en el inicio de la sesión de comunicación entre un punto de acceso y una estación inalámbrica. El inicio de una comunicación comienza por un proceso llamado "asociación."

Cuando el estándar IEEE 802.11b fue diseñado, se introdujeron dos mecanismos de "asociación":

1. *Autenticación abierta:* Implica la **NO** seguridad y cualquiera puede hablarle al punto de acceso.

Por ejemplo; la firma Lucent Tecnhologies desarrolló en el año 2000 una variación del esquema de Autenticación abierta llamado "red cerrada". Las redes cerradas se diferencian del estándar 802.11b en que el punto de acceso no difunda periódicamente las llamadas "Tramas Baliza" o "Beacon Frames".

Evitar la publicación de la SSID implica que los clientes de la red inalámbrica necesitan saber de manera previa qué SSID´s deben asociar con un punto de acceso. Esta cualidad ha sido implantada por muchos fabricantes como una mejora de "seguridad".

2. *Autenticación con clave compartida:* Se comparte una contraseña entre el punto de acceso y la estación cliente.

Por ejemplo: La autenticación con clave compartida implementada en WEP es obsoleta. Varios ataques tipo texto plano, versus texto cifrado, pueden vulnerar la Autenticación basada en WEP. Debido al hecho de que la clave de cifrado y Autenticación son el mismo secreto compartido, una vez que una resulta comprometida, la otra también.

Filtrado de direcciones MAC como medida de seguridad

El filtrado de direcciones MAC utiliza esta dirección para identificar qué dispositivos pueden conectarse a la red inalámbrica. Cuando un cliente inalámbrico intenta conectarse envía la información de la dirección MAC. Si está activado el filtrado MAC, el router inalámbrico buscará la dirección MAC en una lista preconfigurada, de manera que sólo los dispositivos MAC pregrabados en la base de datos podrán conectarse, y si la dirección MAC no se encuentra en la base de datos, el dispositivo no podrá conectarse ni comunicarse a través de la red inalámbrica.

Existen algunos problemas con este tipo de seguridad, por ejemplo: se requiere que se incluyan en una base de datos las direcciones MAC de todos los dispositivos que tendrán acceso a la red antes de que se intente la conexión. Por

lo tanto, no podrá conectarse un dispositivo que no esté identificado en la base de datos; pero es posible que el dispositivo de un atacante clone la dirección MAC de otro dispositivo que tenga el acceso.

6.5.3.3 Integridad de datos en redes inalámbricas

Se define a la integridad de datos como la capacidad de un protocolo inalámbrico para determinar si la información transmitida ha sido alterada por personas no autorizadas.

En 1999 el protocolo WEP buscó proveer integridad de tráfico de datos, pero desafortunadamente el mecanismo de integridad seleccionado el cual fue CRC (Código de Redundancia Cíclica), resultó inseguro. El diseño fallido de WEP permite la alteración del código CRC del tráfico, sin la necesidad de saber la llave WEP, es decir que el tráfico puede ser alterado sin que se note.

Los protocolos WPA y WPA2 resolvieron el problema de la integridad de datos en WEP mediante la inclusión de un mensaje de código de autenticación más seguro y la inclusión de un contador de segmentos (frames), que previene los "ataques por repetición" (replay attack). En un ataque de repetición el atacante registra la conversación entre un cliente y un punto de acceso para obtener un acceso no autorizado. Al responder una conversación "antigua" el atacante no necesita saber la clave secreta WEP.

Por lo tanto se recomienda que se implemente WPA o WPA2 para lograr integridad de datos inalámbrica mediante el cifrado en la capa de enlace.
WPA fue diseñado como un paso intermedio hacia WPA2 (estándar IEEE 802.11i). WPA sólo incluye un subconjunto de las características del estándar IEEE 802.11i y se enfoca en preservar la compatibilidad con adaptadores que funcionan con el estándar IEEE 802.11b.

WPA abordó las fallas encontradas en WEP e incrementó la longitud y el número de las claves en uso, así mismo, agregó un nuevo mensaje de código de autenticación.

6.5.3.4 Disponibilidad en redes inalámbricas

Se define disponibilidad como la capacidad de la tecnología que asegura un acceso confiable a servicios de datos e información para usuarios autorizados, cada que se requiera y cuantas veces sea necesario.

Se considera que no es tan sencillo detener a alguien que busca interferir con su señal de radio ya que las redes inalámbricas operan en canales predefinidos que cualquiera puede usar para enviar señales de radio. Por ello, la prevención de la interferencia por parte de los usuarios no autorizados es prácticamente imposible. Lo único que se puede hacer es monitorear cuidadosamente los enlaces para identificar las fuentes potenciales de interferencia.

Negación de servicio

Las redes inalámbricas son vulnerables a los ataques de Negación de servicio mediante interferencia de radio. Se considera un escenario donde otro operador de red decide configurar sus dispositivos de radio en el mismo canal en el que opera una red.
Para evitar esta clase de ataques, intencionales o no, se debe considerar el rastreo periódico de frecuencias de radio y para evitar la interferencia con otras redes, no hay que sobrecargar la potencia de los enlaces.

Existen varias razones para que un enlace se desempeñe de manera deficiente o no esté disponible, por ejemplo, la presencia de nodos escondidos puede afectar el desempeño de la familia de protocolos IEEE 802.11. Virus, software de intercambio de archivos, “spam”, etc., pueden inundar la red con tráfico y

limitar el ancho de banda disponible para las conexiones autorizadas a servicios legítimos.

6.5.3.5 No repudio (rendición de cuentas)

La familia de estándares IEEE 802.11 no se hace cargo de la "rendición de cuentas" en el tráfico de datos. Los protocolos inalámbricos no tienen un mecanismo para asegurar que el emisor de datos tenga una prueba de envío de la información y que el receptor obtenga una prueba de la identidad del emisor.

En este sentido, cabe destacar que el no repudio es un servicio de seguridad que ofrece protección a un usuario frente a otro que rechace haber realizado cierta emisión de datos o niegue la recepción de un mensaje que le haya sido enviado; esta protección se efectúa por medio de una colección de evidencias irrefutables que regularmente son colectadas por los dispositivos que procesan la transmisión de los datos.

6.5.4 Principales amenazas de seguridad en redes inalámbricas

Resulta interesante conocer el tipo de amenazas a las que se enfrentan las organizaciones hoy en día, por ello en la tabla 6.2 se presentan las principales amenazas de seguridad más relevantes en redes inalámbricas con algunas recomendaciones para cada una de éstas.

Tabla 6.3 Las 10 amenazas más relevantes

	Tipo de Amenaza	Descripción	Solución
1	**Confidencialidad**	Riesgo de interferencia, usuarios no autorizados pueden obtener acceso al tráfico de datos en su red.	- Usar cifrado en la capa de enlace en sus enlaces inalámbricos (WPA2). - Recomendar a sus usuarios el uso de "cifrado" en protocolos de alto nivel (SMTP seguro,

			HTTPS).
2	**Confidencialidad**	Riesgo de arrebato de tráfico y riesgo de un ataque tipo de intermediario.	- Recomendación 1 + - Monitorear la SNR, la SSID y la dirección MAC de su conexión.
3	**Autenticación**	Riesgo de acceso no autorizado a la red inalámbrica	- Implementar IEEE 802.1X (WPA2). - No depender solo de un esquema de autenticación basado en direcciones MAC. - No publicar la SSID.
4	**Autenticación**	Riesgo de acceso no Autorizado a la red inalámbrica y a Internet.	- Implementar IEEE 802.1X - Implementar un portal cautivo.
5	**Integridad**	Riesgo de alteración de tráfico en la red inalámbrica.	- Se recomienda a los usuarios el uso de cifrado en las capas superiores (HTTPS, SMTP seguro). - Usar cifrado en el enlace inalámbrico.
6	**Disponibilidad**	Riesgo de interferencia. Negación de servicio (Congestionamiento)	- Monitorear periódicamente el espectro de radio. - No sobrecargar la potencia de los enlaces.
7	**Disponibilidad**	Riesgo de no disponibilidad de ancho de banda debido a retransmisiones de radio	- Buscar nodos ocultos y fuentes de interferencia- - Monitorear retransmisiones de capa de enlace en puntos de acceso.
8	**Disponibilidad**	Riesgo de no disponibilidad de ancho de banda debido a software malicioso	- Monitorear tráfico IP, especialmente de tipo ICMP y UDP. - Incluir detectores de intrusión.
9	**Autenticación**	Riesgo de acceso no	- Implementar la red inalámbrica fuera de algún firewall.

	Rendición de cuentas	autorizado a Internet.	- Implementar una red privada virtual y permitir conexiones solo vía el concentrador VPN.
10	**(Acceso a la red) Rendición de cuentas**	Riesgo de uso no autorizado de recursos de la red.	- Implementado en IEEE 802.1X - Implementar un portal cautivo basado en firmas digitales.

Es importante generar conciencia sobre la necesidad que existe hoy en día para mantener protegida la información que se encuentra almacenada en los equipos de cómputo. Ya que si bien es cierto, la cantidad de usuarios de Internet ha aumentado considerablemente según un estudio publicado por AMIPCI (Asociación Mexicana de Internet), el cual revela que del año 2007 al 2009 hubo un incremento de internautas de 21.6 millones a 22.7 millones (únicamente tomando en cuenta la zona urbana).[50] Por ello, los usuarios deben conocer las principales amenazas a las que se está expuesto y sobre todo, tener las herramientas que permitan mitigar cualquier anomalía que se pueda presentar.

6.6 Seguridad en bases de datos

Actualmente las bases de datos son herramientas que se utilizan en cualquier aplicación basada en web permitiendo que la interfaz de estos sean dinámicos. Debido a que la información que resulta ser sensible o secreta puede ser almacenada en una base de datos, se vuelve muy importante el hecho de mantenerlas protegidas.

Se define a una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.

[50] http://estudios.amipci.org.mx:8080/mashboard/main.jsp

Entre las principales características de los sistemas de base de datos se pueden mencionar las siguientes:

- Independencia lógica y física de los datos
- Redundancia mínima
- Acceso concurrente por parte de múltiples usuarios
- Integridad de los datos
- Consultas complejas optimizadas
- Seguridad de acceso y auditoría
- Respaldo y recuperación
- Acceso a través de lenguajes de programación estándar

6.6.1 Sistema de Gestión de Base de Datos (SGBD)

Los sistemas de gestión de bases de datos (DataBase Management System) son un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan. Se compone de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta.

Las bases de datos (BDs) nacen con el fin de resolver las limitaciones que en algunos casos presentan los ficheros para el almacenamiento de la información. En los entornos de bases de datos, las diferentes aplicaciones y usuarios utilizan un único conjunto de datos integrado a través de un Sistema de Gestión de Bases de Datos (SGBD). De esta manera se pueden resolver problemas como duplicación de información, inconsistencia de los datos y dependencia entre programa estructura de datos.

Para conseguir un entorno de bases de datos seguro se deben de identificar las amenazas reales así como la adecuada elección de políticas de seguridad que ayuden a establecer mecanismos de prevención como por ejemplo; métodos que comprueben que no se han producido accesos ilícitos.

Una amenaza contra la seguridad de las bases de datos es un agente hostil que puede difundir o modificar información gestionada por el SGBD sin la debida autorización. Las amenazas contra la seguridad se clasifican en:

- **Accidentales:** Pueden ser errores de hardware o software y fallos humanos.
- **Fraudulentas:** Son realizadas intencionalmente por usuarios no autorizados.

Las violaciones que puede sufrir un entorno de bases de datos consisten en lecturas, modificaciones y borrado de datos. Las consecuencias son:

- Difusión de información confidencial
- Modificación no autorizada de datos
- Denegación de servicio a usuarios

6.6.2 Confidencialidad de la BD

En primer lugar el sistema de BD debe identificar y autenticar a los usuarios, además el administrador deberá especificar los privilegios de cada uno sobre los objetos, por ejemplo; utilizar una BD, consultar ciertos datos o actualizarlos.

Para facilitar la administración de los SGBD se suelen incorporar el concepto de perfil, rol o grupo de usuarios que agrupa una serie de privilegios por lo que el usuario que se asigna a un grupo hereda todos los privilegios del grupo.
Por lo tanto, el mecanismo de control de acceso se encarga de denegar o conceder el acceso a los usuarios.

Existen 3 tipos de autorización y son:

1. **Autorización Explícita vs. Implícita:** La primera consiste en almacenar qué sujetos pueden acceder a ciertos objetos con determinados privilegios. La segunda consiste en que una autorización definida sobre un objeto puede deducirse a partir de otras.

2. **Autorización Fuerte vs. Débil:** En la fuerte no se pueden invalidar las autorizaciones implícitas mientras que en la débil se permiten excepciones sobre ellas.
3. **Autorización Positiva vs. Negativa:** La primera indica la existencia de autorización y la segunda indica la denegación de una autorización.

El tipo de autorización que se adopte dependerá entre otras cosas de las políticas de control y de los modelos de datos.
Un punto importante a considerar es que con el cifrado también se obtiene confidencialidad.

6.6.2.1 Deducción de información confidencial de una BD

Las BDs como almacén de gran cantidad de información estructurada pueden ser víctimas de accesos no autorizados con el fin de difundir información confidencial. Existen dos formas de obtener datos de manera ilegal:

1. Consiste en deducir información confidencial utilizando datos que son accesibles (interferencia).
2. La información secreta se consigue combinando varios datos no confidenciales (agregación).

Para proteger las BD de inferencias es conveniente conocer la información de la que se vale el atacante. Dicha información es dependiente de la BD y la aplicación es difícil de obtener. Una regla básica a aplicar es que *el SGBD no debe proporcionar información adicional al atacante.* Así mismo, la BD debe estar organizada de manera que no ayude al atacante, para esto se ha de identificar para cada BD la información a proteger y ajustar los niveles de seguridad requeridos.

Existe otro tipo de deducción y es la *inferencia estadística*, este tipo de deducción se realiza al intentar acceder a las bases de datos estadísticas con el

propósito de obtener datos individuales. Estas bases de datos mantienen información sobre grupos de individuos y deben ser sólo accesibles a través de operaciones estadísticas por ejemplo; media, varianza, entre otros. Sin embargo programadores hábiles pueden intentar acceder a la información individual. Para evitar esto existen dos tipos de protección:

- **Perturbación de los datos:** Se realiza directamente sobre la información protegida. Una vez que se ha identificado y agrupado la información que es considerada de carácter confidencial se reemplazan los datos reales por microestadísticas que conservan el valor global de la BD sin almacenar datos privados. También es posible hacer alteraciones aleatorias entre las tuplas.
- **Control de las preguntas:** La mayor parte de los controles de este tipo se basa en el número de registros a devolver como respuesta a la pregunta. La idea consiste en satisfacer únicamente demandas de información cuyo resultado se encuentra entre unos límites de tamaño con el objetivo de que no se pueda inferir información individual. Esto, aunque ideal, se traduce en un proceso caro y difícil de manejar. Por ejemplo se podría pedir a una BD que nos diese la media de sueldos de los trabajadores de una plantilla (poniendo restricciones: gafas, barba y número de hijos, entre otras.) si sólo hay uno ya se sabe el valor. Pero resulta que la limitación de devolver datos estadísticos si el conjunto al que se refiere es menor que N tampoco es la solución. No lo es porque la combinación de preguntas puede permitir el deducir cosas. Así, si hay 2N empleados siempre se pueden hacer otras preguntas que vayan refinando la información (dame el sueldo de toda la plantilla menos el director) y obtener los valores de los otros 2N-1.

6.6.3 Disponibilidad de la BD

Los SGBD deben asegurar la disponibilidad de los datos a aquellos usuarios que tienen derecho a ello, por lo que proporcionan mecanismos que permiten recuperar las bases de datos contra fallos lógicos o físicos que destruyan la información.

Por lo tanto es conveniente contar con facilidades ajenas al SGBD como, por ejemplo, máquinas tolerantes a fallos, sistemas de alimentación ininterrumpida, entre otros.

Se vuelve importante asegurar la consistencia de los datos tras realizar cambios a la base de datos, para ello, se crean transacciones; éstas se encuentran en un estado consistente antes de que se comience a ejecutar una transacción y también lo deberá estar cuando la transacción termine. Las propiedades principales que debe poseer una transacción son; atomicidad, preservación de la consistencia, aislamiento y persistencia.

- **Atomicidad:** La atomicidad de una transacción garantiza que todas sus acciones sean realizadas o ninguna sea ejecutada, por ejemplo, en el caso de una transacción bancaria o se ejecuta tanto el "depósito-deducción" o ninguna acción será realizada.
- **Preservación de la consistencia:** Muy similar a la "atomicidad", la consistencia garantiza que las que hayan sido declaradas para una transacción sean cumplidas, por ejemplo, (con respecto a una transacción bancaria), suponiendo que cada vez que se realice una transferencia interbancaria de $100,000 sea necesario notificar a la sucursal del tarjeta habiente, si no es posible comunicarse y actualizar la información en la sucursal del cliente, toda la transacción será abortada.
- **Aislamiento:** Garantiza que las transacciones que se estén realizando en el sistema sean invisibles a todos los usuarios hasta que éstas hayan sido declaradas finales. Tomando en cuenta el ejemplo anterior, en la transacción bancaria es posible que el sistema esté programado para intentar en 5 o 10 ocasiones más antes de abortar una transacción por completo, a pesar que este último paso no ha sido finalizado, ya existen otras modificaciones en el sistema, este aislamiento garantiza que los usuarios del sistema no observen estos cambios intermedios hasta que sea finalizada la última acción de actualización.
- **Persistencia:** La durabilidad de una transacción garantiza que al instante en el que se finaliza la transacción ésta perdure a pesar de otras consecuencias, esto es,

si el disco duro falla, el sistema aún será capaz de recordar todas las transacciones que han sido realizadas en el sistema.

Para conseguir anular y recuperar transacciones, el método más extendido suele ser la utilización de un fichero denominado diario (log) en el que se va guardando toda la información necesaria para deshacer o rehacer las transacciones. Normalmente se obliga a que los registros que se modifican se escriban antes en el fichero diario que en la base de datos, para poder anular así, en caso de necesidad, las transacciones y evitar problemas.

Cabe mencionar que si bien los logs son una herramienta de apoyo para la seguridad de la información dado que permiten identificar el tipo de operación realizada sobre las bases de datos, la fecha de realización, el usuario o proceso responsable de dicha acción, entre otros; puede tornarse en un lastre si no se configuran correctamente, esto es, se vuelve necesario realizar un análisis de riesgos a fin de determinar las posibles amenazas a las bases de datos y con base en ello el tipo de información que se debe almacenar en los logs, por otra parte, decidir que todo debe guardarse atenta contra la capacidad de almacenamiento del sistema para este fin, por ejemplo, cuando una contingencia se presenta, se recurre a la revisión de los logs para deslindar responsabilidades y determinar la fuente del ataque, pero el hecho de tener que revisar grandes volúmenes de información sin saber con certidumbre qué buscar, ni en donde, resulta ser un trabajo sin beneficio alguno, provocando así que los ataques se vuelvan a llevar a cabo ya que no se sabe con certeza el origen de éste.

Por otra parte, en la disponibilidad de la BD se puede recurrir a la recuperación de ésta de dos formas:

1. **Recuperación en caliente:** Al ocurrir un fallo que dé lugar a la pérdida de memoria volátil, es preciso realizar la operación de recuperación en caliente, en la que el sistema consulta el fichero diario para determinar las transacciones que hay que deshacer y rehacer.

2. **Recuperación en frío:** En caso de un fallo de memoria secundaria que afecte a la base de datos, se lleva a cabo una recuperación en frío, que consiste en utilizar una copia de seguridad de la BD. La copia de seguridad permitirá, junto con los ficheros diarios que se han ido produciendo desde que se realizó, llevándola de forma consistente a la situación anterior a que se produjera el fallo.

El *error fatal* se produce cuando se pierde el fichero diario grabado en un soporte. En este caso resulta imposible recuperar la base de datos a su estado actual. La mejor solución para evitar este problema es la que ofrecen algunos SGBD, que permiten la gestión de copias de fichero diario en dispositivos independientes, también se puede duplicar la base de datos. En general todas las técnicas de duplicación se conocen como espejo o duplexación.

La técnica espejo requiere de dos servidores de bases de datos que estén comunicados entre sí. En la figura 6.14 se observa la idea básica que muestra dos bases de datos, una primaria y un espejo o copia de la primaria. La primaria es la base de datos operativa sobre la que se ejecutan todas las transacciones, sin embargo a través de procesos automatizados hay un envío constante de los archivos de la bitácora a la base de datos espejo de tal forma que al ocurrir una falla que ponga fuera de operación a la base de datos primaria, se habilite la espejo de forma transparente para los usuarios.

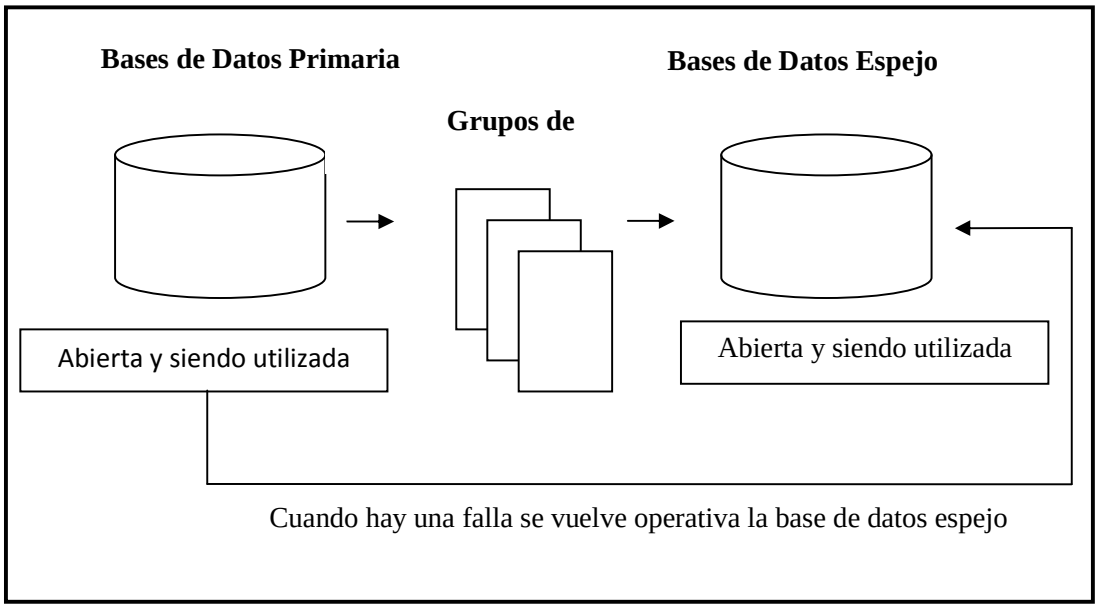


Figura 6.14 Bases de datos espejo

Este ambiente es de alta inversión ya que se necesitan, al menos, dos servidores con las mismas características para albergar las dos bases de datos iguales y una red eficiente que garantice la comunicación 7x24 entre ambos equipos ya que, de otra forma, al haber una falla se estaría igual que en un ambiente normal.

6.6.4 Integridad de la BD

Las vulnerabilidades de la integridad de la BD permiten la modificación, adición o borrado de información de la BD. La integridad se debe garantizar también frente a errores del sistema, virus y sabotajes que puedan dañar los datos almacenados. Este tipo de protección se consigue mediante controles del sistema apropiados, procedimientos de respaldo y recuperación así como procedimientos de seguridad *ad hoc.*

En general se pueden diferenciar dos peligros que requieren tratarse de diferente forma. Por una parte se tiene el problema de la consistencia de los datos debido a errores en el

sistema y por otra los usuarios que pretenden realizar modificaciones no autorizadas en la BD.

Por lo tanto el SGBD debe mantener la consistencia de los datos incluidos en la BD frente a los peligros como la caída del sistema y bloqueo mutuo entre procesos que realizan accesos concurrentes.

Los accesos para realizar modificaciones en la BD son tareas delicadas que la puede dejar inconsistente, por ejemplo, si mientras se está modificando un registro de la BD hay un corte de fluido eléctrico, no se puede tener la seguridad de que se haya quedado grabado en la BD.

Para mantener la consistencia, la SGBD trabaja con **transacciones,** que son unidades de programa que realizan una única función lógica en una aplicación de la BD. Estas transacciones deben de cumplir dos requisitos:

1. Ser atómicas, es decir, todas las operaciones asociadas a una transacción deben ejecutarse por completo o ninguna de ellas.
2. Deben ser correctas, es decir, cada transacción debe ser un programa que conserve la consistencia de la BD.

Por lo tanto, si se produce algún incidente durante la ejecución de una transacción que deje la BD inconsistente, el SGBD debe recuperar el estado previo a dicha transacción.

Los procedimientos de respaldo y recuperación tienen cómo objetivo recuperar un estado anterior de la BD. Para ello, mantienen en un fichero (fichero LOG o bitácora de la BD) información sobre las transacciones que se realizan. Si por cualquier razón se detecta que se pierde la consistencia en la BD el sistema de recuperación deshace las modificaciones realizadas por las últimas transacciones hasta dejar la BD consistente.

Para asegurar la integridad operativa de la BD se ha de controlar la consistencia lógica de los datos cuando se producen transacciones concurrentes. Por ejemplo, cuando un agente desea modificar un registro mientras otro lo está leyendo. Cuando se pueden producir accesos simultáneos a un mismo objeto de la BD la práctica común consiste en bloquear el objeto accedido al tiempo que dure la operación y liberarlo una vez completada.

En cuanto a los intentos de acceso no autorizados para de modificar las BD, las políticas de integridad se basan en limitar los privilegios a los usuarios en cada momento, de tal forma que cada usuario sólo pueda acceder a los datos que precisa para su trabajo, utilizando únicamente las operaciones estrictamente necesarias, por ejemplo:

- Limitar el número de intentos de acceso
- Bloquear la cuenta o el permiso para acceder a la BD si se alcanza el límite máximo de intentos de acceso permitido.
- Enviar una alerta al administrador de la BD

Las restricciones de privilegios no sólo se aplican a departamentos dentro de una organización, sino también a grupos de usuarios con tareas comunes. Una mejora para realizar esto de forma ordenada consiste en utilizar los roles que permiten agrupar usuarios que comparten los mismos privilegios.

Así, el SGBD puede controlar fácilmente las actividades de los usuarios y detectar los cambios en los privilegios otorgados a cada rol (así como se muestra en la figura 6.15). Además, el administrador de la BD puede fácilmente modificar los privilegios a grupos de usuarios cambiando un único rol.

Roles	**Actualizar registro**	**Borrar registro**	**Añadir registro**
Personal	**X**	**X**	**X**
Contabilidad	**X**		
Dirección	**X**	**X**	

Privilegios	**Personal**	**Contabilidad**	**Dirección**
Julen	X		
Martha			**X**
Martín		**X**	

Figura 6.15 Ejemplo de control de acceso basado en roles

6.6.5 Mecanismo de seguridad en SGBD

El SGBD juega un papel crucial en cuanto a la seguridad en una organización. El sistema operativo debe proporcionar ciertos mecanismos de protección básicos; por ejemplo, el sistema operativo ha de garantizar la identidad del usuario y la protección de los ficheros físicos sobre los que está soportada la BD. Por otra parte, el SGBD debe hacerse cargo de restricciones de seguridad dependientes de las aplicaciones y los requerimientos de seguridad principales deben hacer frente a los siguientes aspectos:

a) Acceso a diferentes niveles de gradualidad: En un entorno de BD se puede acceder a los datos a diferentes niveles (BD, colección de relaciones, una relación, conjunto de columnas de una relación, algunas filas de una relación). El SGBD debe establecer controles de acceso a cada nivel de gradualidad.

b) Varios modos de acceso: Los controles de acceso deben ser distintos según la operación a realizar. Por ejemplo; select, insert, update, delete en sql.

c) Diferentes tipos de control de acceso: El acceso se puede regular mediante diferentes tipos de controles: control basado en el nombre del objeto a acceder, control basado en el contenido del objeto a acceder, control dependiente del contexto (ejemplo; permitir o denegar el acceso dependiendo de ciertas variables de entorno como el día, hora o terminal), control dependiente de los procedimientos auxiliares.

d) Autorización dinámica: El SGBD debe ser capaz de modificar las autorizaciones de los usuarios dinámicamente mientras la BD sea operativa.

e) Protección multinivel: Con este método se etiqueta cada objeto de la BD con un nivel de seguridad. Teniendo en cuenta los diferentes niveles de gradualidad dentro de una BD, se puede tener una relación etiquetada con un nivel de seguridad y los atributos de dicha relación tienen su propio nivel de seguridad.

e) Auditoría: Los eventos importantes o sospechosos que se produzcan durante operaciones con la BD deben ser almacenados para su posterior análisis en busca de acciones no autorizadas. Las secuencias de acciones realizadas por un mismo usuario pueden ser utilizadas para detectar posibles inferencias. Esta práctica puede ser un agente disuasorio contra los usuarios que tengan malas intenciones. El

problema de la auditoría consiste en la cantidad de información que se ha de almacenar si se desea controlar las operaciones a un bajo nivel de gradualidad.

Además de estos requerimientos, el SGBD debe asegurarse de que no existan canales ocultos a través de los cuales se pueda divulgar información confidencial así cómo puertas traseras que permitan acceder a usuarios no autorizados. También se debe de controlar el flujo de la información.

Normalmente, el recurso que se utiliza para restringir el acceso a las BD son las vistas, éstas son una forma de proporcionar a cada usuario un modelo personalizado de la BD. Una vista puede ocultar al usuario los datos que no necesita ver y de la misma forma, los datos que tienen el acceso negado. El objetivo de la seguridad se logra si se dispone de un mecanismo que limite a los usuarios a utilizar vistas personales.

Otra medida de seguridad interesante es guardar las tablas de la BD y no dejarlas disponibles a terceros que puedan extraer información de su estructura que luego les sirva para realizar deducciones de la BD. La mejor forma de ocultarlas es mediante cifrado.

Finalmente, un aspecto importante a considerar en los sistemas de información es la eficiencia. Los controles de seguridad conllevan un costo computacional adicional por lo que se debe de generar un compromiso entre mantener el tiempo de respuesta de la BD en límites razonables y la BD segura.

6.7 Ética Informática

La *ética informática* se considera como la disciplina que analiza problemas éticos que son creados por la tecnología de los equipos de cómputo o también los que son transformados o agravados por la misma, es decir, por las personas que utilizan los avances de las tecnologías de la información.

Según Moor la ética informática (EI*) es el análisis de la naturaleza y el impacto social de la tecnología informática y la correspondiente formulación y justificación de políticas para*

un uso ético de dicha tecnología. La tarea de la EI es aportar guías de actuación cuando no hay un reglamento o cuando la que existe se encuentre obsoleta.

Otra definición de la ética informática según Terrel Bynum la define como *la disciplina que identifica y analiza los impactos de las tecnologías de la información en los valores humanos y sociales.* Un ejemplo de este tipo de valores son; la salud, la riqueza, el trabajo, la libertad, la democracia, el conocimiento, la privacidad, la seguridad o la autorrealización personal.

En este concepto la EI quiere incluir términos, teorías y métodos de disciplinas como la ética aplicada, la sociología de las computadoras, la evaluación social de las tecnologías o el derecho informático.
Es importante crear conciencia en nuestra sociedad sobre la tecnología informática y también ayudar a los usuarios que la utilizan, no sólo con eficiencia sino con criterios éticos, cuyo objetivo es tomar decisiones sobre temas tecnológicos de manera consistente con la afirmación de los propios valores o con los derechos humanos en general.

Para ello, esta disciplina plantea algunos objetivos:

- Determinar en qué medida son agravados, transformados o creados por la tecnología informática.
- Analizar y proponer un marco conceptual adecuado y formular principios de actuación para determinar qué hacer en las nuevas actividades ocasionadas por la informática en las que no se perciben con claridad líneas de actuación.
- Realizar análisis éticos de casos realistas y significativos.

- Para realizar lo anterior la EI pretende tener en cuenta dos aspectos:

- Utilizar la teoría ética para clarificar los dilemas éticos y detectar errores en el razonamiento ético.

- Colaborar con otras disciplinas en ese debate, siendo conscientes de los puntos de vista alternativos en las cuestiones referentes a valores y sabiendo discriminar en los distintos casos entre las consideraciones éticas y las técnicas.

6.7.1 Contenidos de la ética informática

- **Ética profesional general:** Hace referencia a problemas que son comunes a otras actividades ocupacionales, por un lado, están los criterios de moralidad personal, entendiendo como tales los criterios, obligaciones y responsabilidades personales de los profesionales. Por otro lado están los problemas interiores a la empresa: relaciones empleador – empleado, lealtad organizacional, interés público, entre otros.
- **La utilización de la información:** El principal problema es el uso no autorizado de los servicios informáticos o de la información contenida en ellos. Se plantean problemas de invasión de la privacidad, de falta de confidencialidad en la información, sobre todo de datos sensibles.
- **Lo informático como nueva forma de bien o propiedad:** Hace referencia al software informático como un bien que tiene características específicas como la piratería, el plagio, los derechos de autor, entre otros.
- **Lo informático como instrumento de actos potencialmente dañinos:** Lo informático es el medio o instrumento por medio del cual se cometen acciones que provocan daño a terceras personas. Los que proveen servicios informáticos y los que utilizan ordenadores, datos y programas han de ser responsables de la integridad y conveniencia de los resultados de sus acciones.

Se puede mencionar de las consecuencias de los errores en datos y algoritmos, los problemas que se pueden causar por la falta de protección en la seguridad de sistemas con datos sensibles o que implican riesgos en la salud de clientes, los actos de terrorismo lógico, las acciones de fanáticos, el espionaje de datos, las introducciones de virus y gusanos.

- **Dimensiones sociales de la informática:** La informática ha contribuido en el desarrollo positivo de los medios de comunicación social, las tecnologías de la información han hecho posible las comunicaciones instantáneas.

La accesibilidad, la distribución equitativa, la justicia social, el trabajo autorrealizante, el crecimiento sostenido, entre otros, son valores que están en juego en la implantación de las nuevas tecnologías.

6.7.2 Código deontológico

La deontología informática trata de la moral o la ética profesional en el manejo del activo más importante que tienen las empresas que es la información. Los profesionales de la informática y las empresas del mundo de las TIC están desarrollando código deontológico para garantizar la conducta ética en las organizaciones.

Elaborar un código de ética es una tarea laboriosa y detallista, lamentablemente muchas asociaciones profesionales y empresas creen que su tarea termina cuando consiguen presentar en sociedad un código ético propio bien elaborado mostrándose así ante sus propios países y ante la comunidad internacional como organizaciones responsables y preocupadas por la ética, sin embargo, hoy en día hay también serios intentos de hacer ver a las asociaciones profesionales que es necesario apoyar activa y continuamente a sus asociados en sus deseos de actuar con justicia en su profesión.

6.7.3 Objetivos del código deontológico

El código deontológico debe establecer las normas de comportamiento para lograr un desempeño de la profesionalidad del mayor nivel posible y dentro de las normas éticas tan necesarias en nuestra actual sociedad.

Un código deontológico intenta alcanzar los siguientes objetivos:

- Determinar las normas de comportamiento para garantizar que se utilizarán buenos modos.
- Hacer prevalecer en todo momento el interés general por delante del particular.
- Definir lo que está bien o lo que está mal.

- Configurar las actitudes mínimas exigibles.
- Canalizar la acción profesional en conformidad con el propio ideal del profesional.

Por lo tanto, el código deontológico debe cumplir las siguientes funciones:

- Servir de instrumento flexible como suplemento a las medidas legales y políticas.
- Servir como concientización pública.
- Dar identidad, estatus y una definición como profesionales.
- Servir como fuente de evaluación pública de la profesión.
- Aumentar la reputación del profesional.
- Aumentar la confianza de la gente.

6.7.4 Funciones del código deontológico

Las asociaciones de profesionales de la informática y algunas empresas relacionadas con ésta han desarrollado códigos de conducta profesional. Estos códigos tienen distintas funciones:

- El que existan normas éticas para una profesión, quiere decir que un profesional no solo es responsable de los aspectos técnicos del producto, sino también de las consecuencias económicas, sociológicas y culturales.
- Sirven como instrumento flexible como suplemento a las medidas legales y políticas, ya que éstas en general van muy lentas, comparadas con la velocidad del desarrollo de las TI.
- Sirven para crear conciencia en los usuarios.
- Tienen una función sociológica ya que dan una identidad a los informáticos como grupo que piensa de una determinada manera; es símbolo de su estatus profesional y parte de su definición como profesionales.
- Sirven como fuente de evaluación pública de una profesión y es un llamado a la responsabilidad, para que la sociedad tenga conocimiento de lo que ocurre en dicha profesión.

- En las organizaciones internacionales estas normas permiten armonizar legislaciones o criterios divergentes existentes en cada país.

6.7.5 Código Deontológico de los Ingenieros Informáticos

Los códigos deontológicos de los Ingenieros informáticos, son códigos de conducta desarrollados por las asociaciones de profesionales de la informática y algunas empresas relacionadas con ésta.

Estos códigos consisten en los siguientes aspectos:

- Un informático no sólo es responsable de los aspectos técnicos del producto, sino también de las consecuencias económicas, sociológicas y culturales del mismo.
- Los códigos sirven de ayuda a los cuerpos legislativos, administrativos y judiciales.
- Sirven como concientización a los usuarios, ya que al crear normas, hace que éstos estén conscientes de los problemas y estimula un debate para designar responsabilidades.
- Es símbolo de su estatus profesional y parte de su definición como profesionales.
- Aumenta la reputación del profesional y la confianza de los usuarios.
- En las organizaciones internacionales estas normas permiten armonizar legislaciones o criterios divergentes existentes (o ausentes, en su caso) en los países individuales.

Por lo antes mencionado, se puede decir que los códigos deontológicos son un paso importante para crear conciencia en las organizaciones y en la sociedad sobre el gran avance tecnológico y de esa manera utilizar la tecnología de manera segura y eficiente puesto que cuenta ya con normas que la respaldan.

6.8 Legislación y delitos informáticos

En la actualidad las computadoras se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino también como medio eficaz para obtener y conseguir información, lo que las ha ubicado en un nuevo medio de comunicación de uso masivo, cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

Este es el panorama del nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que, la informática es hoy una forma de poder social, ya que está disponible tanto para los gobiernos como a los particulares, debido a su rapidez, así como el ahorro de tiempo y energía. Desafortunadamente los usuarios participan en una dinámica sobre lo lícito e ilícito y es ahí donde entra de manera particular el Derecho, para que regule los efectos que pueda provocar una determinada situación y exista un orden dentro de la sociedad.

Por lo antes mencionado, se sabe que los delitos relacionados con los sistemas informáticos han aumentado en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representando así una amenaza para la economía de los países y también para las sociedades. Por ello es necesario que se conozcan las legislaciones de cada país y así enfrentar de la mejor manera posible los delitos informáticos que se efectúen.

6.8.1 Delitos Informáticos

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la OCDE a París en mayo de 1983, *el término delito informático se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.*[51]

[51] Téllez Valdés, Julio, Derecho Informático, 3ª Ed., México, McGraw-Hill, 2004, p.163

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia como la manipulación fraudulenta de las computadoras con fines de lucro, así como la destrucción de programas o datos, el acceso y la utilización indebida de la información, entre otros, son algunas de las estafas relacionadas con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Desafortunadamente los delitos informáticos son difíciles de detectar debido a que los delincuentes en muchas ocasiones no dejan huella de los hechos cometidos para llevar a cabo su objetivo, en ese sentido, la informática reúne algunas características que la convierten en un medio idóneo para la ejecución de diversos delitos, en especial los de carácter patrimonial (estafas, apropiaciones indebidas, entre otros). Esto es debido a la gran cantidad de datos que se acumulan, por consiguiente resulta fácil acceder a ellos y manipularlos.

Los Delitos informáticos que se cometen con mayor frecuencia son:

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, entre otros).
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de los delitos convencionales (robo, homicidio y fraude).
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.
- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.
- Daño a la memoria.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (como por ejemplo pago de rescate).
- Acceso no autorizado: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
- Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.
- Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.
- Estafas electrónicas: A través de compras realizadas haciendo uso de la red.
- Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

Por otro lado, la red de Internet permite dar soporte para la ejecución de otro tipo de delitos, cómo lo son:

- **Espionaje:** Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- **Terrorismo:** Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

- **Narcotráfico:** Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- **Otros delitos:** Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

Actualmente, los flujos de información o fuentes, como redes de información y medios de radiodifusión, han trascendido y actúan en forma débil cuando deben responder a los principios éticos y morales.

El delito informático implica actividades criminales que los países han definido cómo robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, cabe destacar que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, por ello se vuelve necesario tener una norma por parte del Derecho que lo regularice.

6.8.2 Tipos de Delitos Informáticos

La Organización de Naciones Unidas (ONU) reconoce los siguientes tipos de delitos informáticos:

- Fraudes cometidos mediante manipulación de computadoras.
- Manipulación de los datos de entrada.
- Daños o modificaciones de programas o datos computarizados.

Delincuente y Víctima

- **Sujeto Activo:** Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible.

- **Sujeto Pasivo:** El sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. En el caso de los delitos informáticos las victimas pueden ser individuos, instituciones crediticias, gobiernos u otros que utilicen las tecnologías de información.

6.7.3 Legislación Internacional

A continuación se dan a conocer las diferentes legislaciones que existen en algunos países como Alemania, Austria, Chile, China, España, Estados Unidos, Francia, Holanda e Inglaterra, de tal manera que se haga frente a la delincuencia informática y evitar en la medida de lo posible que se disminuyan este tipo de delitos.

Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra la Criminalidad Económica.

Esta ley reforma el Código Penal (Art. 148 del 22 de diciembre de 1987) para contemplar los siguientes delitos:

- Espionaje de datos (202a).
- Estafa informática (263a).
- Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273).
- Alteración de datos (303a) es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.
- Sabotaje informático (303b).

- Destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b).
- Por lo que se refiere a la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita. Esta solución fue también adoptada en los Países Escandinavos y en Austria.

Austria

Según la Ley de reforma del Código Penal del 22 de diciembre de 1987, se contemplan los siguientes delitos:

- Destrucción de datos (Art. 126) no solo datos personales sino también los no personales y los programas.
- Estafa informática (Art. 148) se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Chile

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos. La ley 19223 publicada en el Diario Oficial (equivalente del Boletín Oficial argentino) el 7 de junio de 1993 señala que la destrucción o inutilización de un sistema de tratamiento de información puede ser castigado con prisión de un año y medio a cinco.

Como no se estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. Si esa acción afectara los datos contenidos en el sistema, la prisión se establecería entre los tres y los cinco años.

El hacking, definido como el ingreso en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en éste, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito.

Dar a conocer la información almacenada en un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años. Esta ley es muy similar a la inglesa aunque agrega la protección a la información privada.

China

El Tribunal Supremo Chino castigará con la **pena de muerte** el espionaje desde Internet, según se anunció el 23 de enero de 2001.
Todas las personas "implicadas en actividades de espionaje", es decir que "roben, descubran, compren o divulguen secretos de Estado" desde la red podrán ser condenadas con penas que van de diez años de prisión hasta la muerte.

La corte determina que hay tres tipos de actividades donde la vigilancia será extrema: secretos de alta seguridad, los secretos estatales y aquella información que dañe seriamente la seguridad estatal y sus intereses. Se consideran actividades ilegales la infiltración de documentos relacionados con el Estado, la defensa, las tecnologías de punta, o la difusión de virus informático.

El Tribunal ha hecho especial énfasis al apartado del espionaje desde la red. A los llamados "criminales", además de tener asegurada una severa condena (la muerte), también se les puede confiscar los bienes.

España

Este país quizás sea el que mayor experiencia ha obtenido en casos de delitos informáticos, en Europa.

Su actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP) aprobada el 15 de diciembre de 1999, la cual reemplaza una veintena de leyes anteriores de la misma índole, contempla la mayor cantidad de acciones lesivas sobre la información.

Se sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el phreacking, la introducción de virus, etc.; aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos.

Así mismo su nuevo Código Penal establece castigos de prisión y multas "a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

Estados Unidos

El primer abuso de una computadora se registró en 1958 mientras que en 1966 se llevó adelante el primer proceso por la alteración de datos de un banco de Mineapolis. En la primera mitad de la década del 70, mientras los especialistas y criminólogos discutían si el delito informático era el resultado de una nueva tecnología o un tema específico, los ataques computacionales se hicieron más frecuentes. Para acelerar las comunicaciones, enlazar compañías, centros de investigación y transferir datos, las redes debían (y deben) ser accesibles, por eso el Pentágono, la OTAN, las universidades, la NASA, los laboratorios industriales y militares se convirtieron en el blanco de los intrusos.

Pero en 1976 dos hechos marcaron un punto de inflexión en el tratamiento policial de los casos: el FBI dictó un curso de entrenamiento para sus agentes acerca de delitos informáticos y el Comité de Asuntos del Gobierno de la Cámara presentó dos informes que dieron lugar a la Ley Federal de Protección de Sistemas de 1985.

Esta ley fue la base para que Florida, Michigan, Colorado, Rhode Island y Arizona se constituyeran en los primeros estados con legislación específica, anticipándose un año al dictado de la Computer Fraud y Abuse Act de 1986.

Éste se refiere en su mayor parte a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales. También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada. Pero sólo es aplicable en casos en los que se verifiquen daños cuyo valor supere el mínimo de mil dólares.

En 1994 se adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030), modificando el Acta de 1986. Aquí se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos.

Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, esta ley es un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos.

El aumento en la cantidad de casos de hacking y la sensación de inseguridad permanente que generaron (fomentada por la difusión de los hechos en programas especiales de televisión y artículos de revistas especializadas), cambiaron la percepción de las autoridades con respecto a los hackers y sus ataques. Los casos que demostraron

ese cambio fueron los del "Cóndor" Kevin Mitnicky y los de "ShadowHawk" Herbert Zinn hijo.

El FCIC (Federal Computers Investigation Comité), es la organización más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales, los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente. El FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional.

Además existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), quien investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias. Sus integrantes son "forenses de las computadoras" y trabajan, además de los Estados Unidos, en el Canadá, Taiwán e Irlanda.

Francia

Aquí, la Ley 88/19 del 5 de enero de 1988 sobre el fraude informático contempla:

- Acceso fraudulento a un sistema de elaboración de datos. Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje Informático. Falsificar el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos. Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados. Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Holanda

Hasta el día 1 de marzo de 1993, día en que entró en vigencia la Ley de Delitos Informáticos, Holanda era un paraíso para los hackers. Esta ley contempla con artículos específicos sobre técnicas de Hacking y Phreacking.

El sólo hecho de entrar en una computadora en la cual no se tiene acceso legal ya es delito y puede ser castigado hasta con seis meses de cárcel. Si se usó esa computadora hackeada para acceder a otra, la pena sube a cuatro años aunque el crimen, a simple vista, no parece ser peor que el anterior. Copiar archivos de la máquina hackeada o procesar datos en ella también conlleva un castigo de cuatro años en la cárcel. Publicar la información obtenida es ilegal si son datos que debían permanecer en secreto, pero si son de interés público es legal.

El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel de seis meses a quince años, aunque el máximo está reservado para quienes causaron la muerte de alguien con su accionar. Cambiar, agregar o borrar datos puede ser penalizado hasta con dos años de prisión pero, si se hizo vía remota aumenta a cuatro.
Los virus están considerados de manera especial en la ley. Si se distribuyen con la intención de causar problemas, el castigo puede llegar hasta los cuatro años de cárcel; si simplemente se "escapó", la pena no superará el mes.

El usar el servicio telefónico mediante un truco técnico (Phreacking) o pasando señales falsas con el objetivo de no pagarlo puede recibir hasta tres años de prisión. La venta de elementos que permitan el Phreaking se castiga con un año de prisión como tope y si ese comercio es el modo de ganarse la vida del infractor, el máximo aumenta a tres. La ingeniería social también es castigada con hasta tres años de cárcel.

Recibir datos del aire es legal (transmisiones satelitales), siempre y cuando no haga falta un esfuerzo especial para conseguirlos; la declaración protege datos encriptados,

como los de ciertos canales de televisión satelital. Falsificar tarjetas de crédito de banca electrónica y usarlas para obtener beneficios o como si fueran las originales está penado con hasta seis años.

Inglaterra

Luego de varios casos de hacking surgieron nuevas leyes sobre delitos informáticos. En agosto de 1990 comenzó a regir la Computer Misuse Act (Ley de Abusos Informáticos) por la cual cualquier intento, exitoso o no de alterar datos informáticos con intención criminal se castiga con hasta cinco años de cárcel o multas sin límite.

El acceso ilegal a una computadora contempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas. El delito se divide en tres partes: hackear (ingresar sin permiso en una computadora), hacer algo con la computadora hackeada y realizar alguna modificación no autorizada.

El último apartado se refiere tanto al hacking (por ejemplo, la modificación de un programa para instalar un backdoor), la infección con virus o, yendo al extremo, a la destrucción de datos como la inhabilitación del funcionamiento de la computadora.

Otras legislaciones

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los

códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún."[52]

En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin e luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".
Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas".[53]

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define **Delito Informático** como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos."[54]

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma".[55]

[52] TÉLLES VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México. 1996 Pág. 103-104
[53] MOLINER, María. Diccionario de María Moliner Edición Digital. Copyright© 1996 Novel Inc.; Copyright © 1996 María Moliner.
[54] Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en Mayo de 1993.
[55] CARRION, Hugo Daniel. Tesis "Presupuestos para la Punibilidad del Hacking". Julio 2001.

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos:

1. Esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.
2. La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

En este punto debe hacerse un punto y notar lo siguiente:

- No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.
- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.
- La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.
- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.
- La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

Julio Téllez Valdez clasifica a los delitos informáticos con base en dos criterios:

1. Como instrumento o medio: se tienen a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

   Ejemplos:

   - Falsificación de documentos vía computarizada: tarjetas de créditos, cheques, entre otros.
   - Planeamiento y simulación de delitos convencionales como robo, homicidio y fraude.
   - Alteración el funcionamiento normal de un sistema mediante la introducción de código extraño al mismo: virus, bombas lógicas, entre otros.
   - Intervención de líneas de comunicación de datos o teleprocesos.

2. Como fin u objetivo: se enmarcan las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

   Ejemplos:

   - Instrucciones que producen un bloqueo parcial o total del sistema.
   - Destrucción de programas por cualquier método.
   - Atentado físico contra la computadora, sus accesorios o sus medios de comunicación.
   - Secuestro de soportes magnéticos con información valiosa, para ser utilizada con fines delictivos.
   - Este mismo autor sostiene que las acciones delictivas informáticas presentan las siguientes características:
     a) Sólo una determinada cantidad de personas (con conocimientos técnicos por encima de lo normal) pueden llegar a cometerlos.

b) Son conductas criminales del tipo "cuello blanco": no de acuerdo al interés protegido (como en los delitos convencionales) sino de acuerdo al sujeto que los comete. Generalmente este sujeto tiene cierto status socioeconómico y la comisión del delito no puede explicarse por pobreza, carencia de recursos, baja educación, poca inteligencia, ni por inestabilidad emocional.
c) Son acciones ocupacionales, ya que generalmente se realizan cuando el sujeto atacado se encuentra trabajando.
d) Son acciones de oportunidad, ya que se aprovecha una ocasión creada por el atacante.
e) Provocan pérdidas económicas.
f) Ofrecen posibilidades de tiempo y espacio.
g) Son muchos los casos y pocas las denuncias, y todo ello por la falta de regulación y por miedo al descrédito de la organización atacada.
h) Presentan grandes dificultades para su comprobación, por su carácter técnico.
i) Tienden a proliferar, por lo se requiere su urgente regulación legal.

María Luz Lima, por su parte, presenta la siguiente clasificación de "delitos electrónicos"[56]:

1. **Como Método:** conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
2. **Como Medio:** conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.
3. **Como Fin:** conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

[56] *LIMA de la LUZ, María. Criminalia N° 1-6 Año L. Delitos Electrónicos. Ediciones Porrúa. México. Enero-Julio 1984.*

Por lo tanto se puede concluir que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, se vuelve importante establecer tratados o acuerdos entre países que ayuden a fijar mecanismos para contrarrestar de manera eficaz los incidentes sobre los delitos informáticos. Así mismo las sociedades harán conciencia sobre lo importante que es mantener protegida la información y si se llega a abusar de ello, tener una norma que castigue los crímenes que se llegasen a cometer.

Conclusiones

A lo largo de este trabajo de investigación se pudo observar un panorama general de la seguridad informática, se dieron a conocer datos muy interesantes que reflejan la situación de nuestro país y del exterior, cumpliendo con los objetivos planteados al inicio de éste.

Como se apreció en el capítulo 1, a lo largo de la historia de las tecnologías de la información se apreció que en las diferentes épocas la preocupación del hombre ha sido y seguirá siendo, mantener protegida su información ante cualquier amenaza que la pudiese poner en peligro. Dada esta situación, se ha buscado la manera de optimizar su almacenamiento y su integridad apoyándose en los avances tecnológicos que se han suscitado a través de los años.

Como se ha visto, en las últimas dos décadas el desarrollo de la tecnología se ha acelerado a pasos agigantados, como en el caso de las computadoras, el Internet, los dispositivos móviles, entre otros. Todo esto ha tenido enormes beneficios para la sociedad, ya que ahora no solo se puede acceder a la información a través de las computadoras, sino que también por medio de los dispositivos móviles y ello ha facilitado la comunicación entre personas no importando el lugar físico en el que se encuentren y por ello, se ha logrado que muchos

países continúen desarrollándose obteniendo un mejor índice de competitividad, por ejemplo, en lo que respecta a Latinoamérica, Chile ocupa el primer lugar ubicándose en el sitio 30, seguido de Puerto Rico con el sitio 42; y los países que ocupan los primeros lugares a nivel mundial son; Suiza, Estados Unidos, Singapur, Suecia y Dinamarca.

México es un país que ha ido creciendo lentamente en cuanto al desarrollo tecnológico, desafortunadamente en épocas anteriores, no se prestaba la suficiente atención sobre la importancia de crear tecnología, ahora ante la nueva era de los dispositivos móviles, se vuelve necesario proteger la información que se encuentra almacenada en estos, debido a que también se convierte en un factor vulnerable de padecer algún tipo de amenaza que atente contra la información almacenada en el dispositivo.

Por ello, se vuelve importante prestar la atención que se merece y crear conciencia sobre la importancia que tiene, de tal manera que sería conveniente que el Gobierno de México invierta en más recursos para que todas aquellas personas que tengan acceso a internet adquieran los conocimientos adecuados para crear una nueva cultura sobre tecnologías y seguridad informática.

Como se observó en el Capítulo 2, paralelo a este avance tecnológico las amenazas y vulnerabilidades se han incrementado considerablemente debido a que existen personas que por diversión o por algún objetivo en particular se dedican a robar, alterar e incluso denegar la información que viaja a través de los equipos de comunicación.

La mayoría de las amenazas y vulnerabilidades que existen a nivel nacional e internacional según los datos analizados por las diferentes empresas de seguridad son el m*alware, spam y el phishing*, posicionando a Estados Unidos como el principal país que padece este tipo de amenazas seguido de China, Brasil, Turquía, Alemania, Taiwán, entre otros.
También se dieron a conocer las principales herramientas de seguridad informática y sus características, cuyo objetivo es proteger, eliminar y prevenir los diferentes tipos de ataques que existen actualmente. Por lo que, se vuelve importante que los usuarios de nuestro país

adquieran los conocimientos sobre este tipo de ataques y así evitar en la medida de lo posible ser víctima de cualquier tipo de delito cibernético.

Por ello es necesario que se cuente con un sistema de seguridad acorde a las necesidades tanto para las empresas como de los usuarios particulares, ya que las primeras son el punto débil de los hackers por el sólo hecho de manejar información delicada, como por ejemplo; nóminas, transferencias electrónicas, información confidencial de los trabajadores, entre otros.

En el Capítulo 3, se dieron a conocer las tendencias de la seguridad informática a nivel nacional e internacional. En el caso de México se observó que se encuentra en el lugar 64 a nivel mundial con respecto al índice de Competitividad, lo que implica que aún se encuentra alejado de posicionarse en un país desarrollado como lo es el caso de Suiza, Estados Unidos, Singapur, Suecia, entre otros. Las principales fallas que se detectaron es la falta de inversión en tecnología, así como los robos, crímenes, corrupción, ineficiencia burocrática, entre otros.

Vimos que se espera que para el año 2020 México ocupe el lugar 20 respecto al índice de competitividad apoyándose de las Tecnologías de la Información, que los ciudadanos se involucren en la toma de decisiones económicas, políticas, sociales y culturales por medio del uso de las TIC’s y que se mantenga una república conectada mediante el uso de éstas.

Por ello me parece importante señalar que la base para obtener un mejor desarrollo se centra en la educación ya que si se invierte lo suficiente, las futuras generaciones tendrán los conocimientos y las herramientas adecuadas para enfrentar los problemas que tiene nuestro país para así, eliminar los huecos existentes para que México se desarrolle y logre estar a la altura de países posicionados en los primeros lugares.

Como se ha mencionado anteriormente, se dieron a conocer las tendencias de las TIC’s, los retos señalados, la proyección que se tiene y en esa medida la seguridad informática continuará siendo una necesidad, ya que permitirá garantizar en la medida de lo posible,

proteger la información y continuar desarrollándose paralelo a los avances tecnológicos que tenga nuestro país.

En el capítulo 4 se realizó un análisis de los planes de estudio de las principales carreras que imparte la Universidad Nacional Autónoma de México. Se observó que la mayoría de las facultades cuenta con un Centro de Cómputo en el cual se brindan los servicios de préstamo de equipo de cómputo, acceso a Internet, correo electrónico, impresiones, cursos de paquetería de office y relacionados con la carrera.
Por ello es recomendable que en los centros de cómputo se impartan asesorías e incluso cursos sobre la Seguridad Informática, de manera que los estudiantes adquieran los conocimientos básicos sobre ésta y sobre todo que se cree una conciencia sobre la importancia de salvaguardar la información, para que de esa manera aprovechen mejor los recursos que se les brinda para su desarrollo profesional.

Para finalizar el presente trabajo, se presentan dos propuestas; en el Capítulo 5 la propuesta sobre el planteamiento de un modelo educativo en materia de Seguridad Informática, llevándose a cabo un análisis general de la situación en la que se encuentran los diferentes niveles educativos y lo que se esperaría en un futuro a corto plazo, de tal manera que se pudiesen detectar las carencias existentes y en base en ello se propuso que los alumnos de los distintos niveles educativos adquieran los conocimientos adecuados para la comprensión de la importancia de la Seguridad de la Información.

Todo esto se realizó con la finalidad de crear una cultura informática y en esa medida, eficientar el uso de los diversos dispositivos que existen actualmente. De esta manera se logrará que los estudiantes tanto de los diferentes niveles educativos, como de las diversas carreras, egresen lo suficientemente capacitados para evitar que continúen siendo víctimas de las amenazas que existen actualmente.
Si bien es cierto, actualmente las empresas son quienes se enfrentan a las principales amenazas cibernéticas, pero hay que reflexionar que esto se debe a diversos factores, como por ejemplo, al incremento tecnológico, a la falta de conocimiento sobre el manejo de éste, a la falta de personal capacitado y especializado en seguridad informática, a la falta de

presupuesto educativo, entre otros. Afortunadamente después de muchos años, se comienza a trabajar en ello, realizando proyectos educativos que permita que los alumnos tengan una mejor enseñanza, apoyándolos con aulas, equipos de cómputo, acceso a Internet gratuito, capacitación del personal adecuado, entre otros.

Por ello, sería recomendable que se anexaran contenidos en los planes de estudio sobre temas de seguridad de la información y que se capacitaran a los profesores para la impartición de dichos temas. También que se cuente con material de apoyo como libros, apuntes, boletines, revistas, equipos de cómputo, internet, talleres, entre otros.

Después de realizar todo un análisis y de la propuesta planteada para impulsar la seguridad informática en cuanto a educación y desarrollo tecnológico, agrego una segunda propuesta que beneficia de manera particular a los estudiantes de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México, para la carrera de Ingeniería en Computación, la cual consistió en la actualización del material de apoyo relacionado con las asignaturas de Seguridad Informática I y II. Estos contenidos se han desarrollado y revisado para que los estudiantes de esta Facultad continúen con una preparación adecuada acorde a los tiempos tecnológicos que se están viviendo en nuestro país y en esa medida adquieran las herramientas necesarias para enfrentar los retos que el país demanda.

Por último en el Capítulo 6, agregué los contenidos de los temas que consideré necesarios sobre la seguridad informática y así colaborar en la educación de los futuros profesionistas, despertando en ellos, el interés sobre lo importante que se vuelve el hecho de mantener protegida la información y que de esa manera lo apliquen no sólo en el lugar que laboren, sino en su vida cotidiana.

Considero que para lograr que México sea un país competitivo es necesario invertir en la educación ya que ésta es la base para el crecimiento y desarrollo de nuestro país.

Finalmente considero que los objetivos planteados en este trabajo de investigación se cumplieron satisfactoriamente. Se espera que la propuesta del modelo educativo sea analizada por el Gobierno de México a través de la Secretaría de Educación Pública y así colaborar para que México tenga una educación gratuita de calidad.

Anexo 1

Plan de estudios 2009

Educación Primaria

MAPA CURRICULAR DE LA EDUCACIÓN BÁSICA

CAMPOS FORMATIVOS PARA LA EDUCACIÓN BÁSICA	PREESCOLAR			PRIMARIA						SECUNDARIA		
	1°	2°	3°	1°	2°	3°	4°	5°	6°	1°	2°	3°
Lenguaje y comunicación	Lenguaje y comunicación			Español						Español I, II y III		
			Asignatura Estatal: lengua adicional***	Asignatura Estatal: lengua adicional***						Lengua extranjera I, II y III		
Pensamiento matemático	Pensamiento matemático			Matemáticas						Matemáticas I, II y III		
Exploración y comprensión del mundo natural y social	Exploración y conocimiento del mundo			Exploración de la Naturaleza y la Sociedad*		Ciencias Naturales*				Ciencias I (énfasis en Biología)	Ciencias II (énfasis en Física)	Ciencias III (énfasis en Química)
										Tecnología I, II y III		
	Desarrollo físico y salud					Estudio de la Entidad donde Vivo*	Geografía*			Geografía de México y del Mundo	Historia I y II	
							Historia*			Asignatura Estatal		
Desarrollo personal y para la convivencia	Desarrollo personal y social			Formación Cívica y Ética**							Formación Cívica y Ética I y II	
										Orientación y Tutoría I, II y III		
				Educación Física**						Educación Física I, II y III		
	Expresión y apreciación artística			Educación Artística**						Artes: Música, Danza, Teatro o Artes Visuales		

* Incluyen contenidos del campo de la tecnología. ** Se establecen vínculos formativos con Ciencias Naturales, Geografía e Historia. *** En proceso de gestión.

Fuente: http://basica.sep.gob.mx/dgdc/sitio/pdf/inicio/matlinea/primer_grado.pdf

Anexo 2

Plan de estudios 2006

Educación Secundaria

Mapa curricular

Primer grado	Horas	Segundo grado	Horas	Tercer grado	Horas
Español I	5	Español II	5	Español III	5
Matemáticas I	5	Matemáticas II	5	Matemáticas III	5
Ciencias I (énfasis en Biología)	6	Ciencias II (énfasis en Física)	6	Ciencias III (énfasis en Química)	6
Geografía de México y del Mundo	5	Historia I	4	Historia II	4
		Formación Cívica y Ética I	4	Formación Cívica y Ética II	4
Lengua Extranjera I	3	Lengua Extranjera II	3	Lengua Extranjera III	3
Educación Física I	2	Educación Física II	2	Educación Física III	2
Tecnología I*	3	Tecnología II*	3	Tecnología III*	3
Artes (Música, Danza, Teatro o Artes Visuales)	2	Artes (Música, Danza, Teatro o Artes Visuales)	2	Artes (Música, Danza, Teatro o Artes Visuales)	2
Asignatura Estatal	3				
Orientación y Tutoría	1	Orientación y Tutoría	1	Orientación y Tutoría	1
Total	**35**		**35**		**35**

Fuente: http://basica.sep.gob.mx/dgdc/sitio/pdf/inicio/matlinea/PlanEstudio06.pdf

A

Administrador de redes: Los administradores de red son básicamente el equivalente de red de los administradores de sistemas: mantienen el hardware y software de la red. Esto incluye el despliegue, mantenimiento y monitoreo de la red: swhitches, routers, firewalls, entre otros.

Adware: Es cualquier programa que automáticamente se ejecuta, muestra o baja publicidad web a la computadora después de instalar el programa o mientras se está utilizando la aplicación.

Acceso remoto: Se refiere a la funcionalidad de algunos programas que permiten realizar ciertos tipos de acciones desde un equipo local y que las mismas se ejecuten en otro equipo remoto.

Active X: Tecnología de software desarrollada por Microsoft para incluir aplicaciones en páginas HTML.

ALAPSI: Asociación Latinoamericana de Profesionales en Seguridad Informática.

AltaVista: Es un buscador en inglés y español de la empresa Overture Service Inc. Comprada a su vez por Yahoo!.

Amenaza: Anuncio de un mal o peligro.

Amenaza lógica: Se refiere a una variedad de programas que de una u otra forma pueden dañar los sistemas creados de manera intencionada o simplemente por error.

Amazon: Compañía estadounidense de comercio electrónico con sede en Seattle, Estado de Washington.

AMIPCI: Asociación Mexicana de Internet

AMITI: Asociación Mexicana de la Industria de Tecnologías de Información.

Análisis de riesgo: Proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentras expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Anomalía: Cambio o desviación respecto de lo que es normal, regular, natural o previsible: *una anomalía cromosómica es cualquier alteración o cambio que se produzca tanto en uno de los cromosomas como en el número de estos en un individuo.*

Antivirus: Programa para prevenir y proteger contra infecciones de virus informáticos, también los elimina y repara algunos de los daños causados.

Apple Computer: Es una empresa multinacional estadounidense que diseña y produce equipos electrónicos y software.

Archivo adjunto: Archivo que se envía junto a un mensaje de correo electrónico.

ARPA: Advanced Research Project Agency.

ARPANET: Advanced Research Projects Agency Network.

Arroba: En informática se utiliza para indicar "en" (at en inglés) en las direcciones de correo electrónico y otros servicios en línea que utilizan el formato usuario@servidor.

Ataque: Intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red.

Ataque cibernético: Acción de causar daño a los sistemas electrónicos.

ATM: Modo de Transferencia Asíncrona (Asynchronous Transfer Mode)

Auditoria: Proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos y cumple con las leyes y regulaciones establecidas.

Aula digital: Concepto dual que adquiere dos significados a nivel físico y virtual. El nivel físico es un espacio para el aprendizaje con alta tecnología, donde la plataforma tecnológica de cómputo y telecomunicaciones posibilitan el desarrollo de nuevas formas y escenarios de aprendizaje. Sobre el nivel físico se desarrolla un espacio y tiempo digital perceptible, llamado espacio virtual; donde las posibilidades de escenarios para el aprendizaje, es sólo limitado por la imaginación de los profesores, estudiantes e ingenieros.

Autenticación: Es el proceso de detectar y comprobar la identidad de una entidad de seguridad mediante credenciales del usuario y la validación de las mismas consultado a una autoridad determinada.

Autopista de la Información: Al Gore acuña la expresión "autopista de la información" para referirse a lo que las computadoras harán en el futuro.

Avatar: En internet y otras tecnologías de comunicación, se denomina "avatar" a una representación gráfica, generalmente humana, que se asocia a un usuario para su identificación. Los avatares pueden ser fotografías o dibujos artísticos.

B

Backdoors (puerta trasera): Es una secuencia especial dentro del código de programación mediante la cual se puede evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema.

Banda ancha: Se refiere a la transmisión de datos en la cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión efectiva. En ingeniería de redes este término se utiliza también para los métodos en donde dos o más señales comparten un medio de transmisión.

Bases de datos: Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Beagle (Gusano): Programa que se reproduce por sí mismo, que puede viajar a través de las redes utilizando los mecanismos de éstas y que no requiere respaldo de software o hardware.

Binario: Sistema de numeración en el que los números se representan utilizando solamente las cifras cero y uno.

Biometría informática: Es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo para verificar identidades o para identificar individuos.

Bit: Es una unidad de información, la más pequeña y se representa con los valores de 0 y 1.

Blacberry: Línea de teléfonos inteligentes (smartphones) que integran el servicio de correo electrónico móvil.

Blaster: Es un gusano que solo afecta a ordenadores con sistemas operativos Windows.

Blog: Sitio web periódicamente actualizado que recopila cronológicamente textos o artículos de uno o varios autores, apareciendo primero el más reciente, donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente.

Bombas lógicas: Partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas.

Borrado de huellas: Se produce después de que ocurrió una intrusión y responde a la necesidad de ocultar los rastros que el intruso haya podido dejar en el sistema atacado.

Botnets: Hace referencia a un conjunto de robots informáticos o bots que se ejecutan de manera autónoma y automática. El Botnet puede controlar todos los ordenadores o servidores infectados de forma remota.

Broadcast storm: Es una condición donde los dispositivos en una red están generando principalmente tráfico Broadcast para que el rendimiento de la red se degrade drásticamente llegando en ocasiones a la pérdida total de la operatividad de la red.

Broadcasting: Término inglés que designa generalmente la emisión de señales de radio y televisión para uso público generalizado o muy amplio.

Brute force: En criptografía se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

Buffer: Dispositivo de memoria que almacena temporalmente los datos enviados a los periféricos.

Bug (Agujero): Defecto o error en una máquina o programa.

Byte: Conjunto formado por 4, 6 u 8 dígitos binarios o bits, que constituye la unidad de transmisión de información: cada byte puede combinarse de 256 formas.

C

Canal de comunicación: Medio de transmisión por el que viajan las señales portadoras de la información emisor y receptor.

Caballo de Troya: Programa que se hace pasar por uno válido cuando en realidad es un programa malicioso.

CCMP: "Counter-Mode/CBC-Mac"

CERN: Organización Europea para la Investigación Nuclear.

CERT: Computer Emergency Readiness Team

Certificación: Garantía que asegura la certeza o autenticidad e algo.

Certificado digital: Documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entra la identidad de un sujeto o entidad y su clave pública.

CFE: Comisión Federal de Electricidad.

Chat: Nombre que proviene del servicio Internet Realy Chat (charla en grupo de internet). Es una forma de conversar en Internet en la que muchos usuarios a la vez hablan y discuten sobre un tema.

Chip: Circuito integrado, montado sobre un aplaca de silicio, que realiza varias funciones en los ordenadores y dispositivos electrónicos.

Ciberespacio: Término utilizado originalmente en la novela "Neuromante" de Willian Gibson, sobre redes de equipos informáticos en el cerebro. Se refiere al campo colectivo de la comunicación asistida mediante equipos informáticos.

Ciberdelincuencia: Se entiende por ciberdelincuencia o delito informático aquellas acciones que han sido cometidas mediante la utilización de un bien o servicio informático, sin dejar a un lado que un sistema informático también es un bien jurídico que recibe protección por parte del ordenamiento jurídico.

Cibernético: Ciencia que estudia la construcción de sistemas electrónicos y mecanismos a partir de su comparación con los sistemas de comunicación y regulación automática de los seres vivos.

CICESE: Centro de Investigación Científica y de Educación Superior de ensenada, BC.

Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Cinta magnética: Tipo de medio o soporte de almacenamiento de información que se graba en pistas sobre una banda plástica con un material magnetizado, generalmente óxido de hierro o algún cromato. El tipo de información que se puede almacenar en las cintas magnéticas es variado, como video, audio y datos.

Circuito: Conjunto de conductores que recorre una corriente eléctrica.

CISCO Systems: Empresa multinacional con sede en (California, Estados Unidos), principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones tales como: dispositivos de conexión para redes informáticas: routers (enrutadores, encaminadores o ruteadores), switches (conmutadores) y hubs (concentradores). Dispositivos de seguridad como cortafuegos y concentradores para VPN. Productos de telefonía IP como teléfonos y el CallManager (una PBX IP). Software de gestión de red como CiscoWorks y equipos para redes de área de almacenamiento.

Cliente: Es el que inicia un requerimiento de servicio. El requerimiento inicial puede convertirse en múltiples requerimientos de trabajo a través de redes LAN o WAN. La ubicación de los datos o de las aplicaciones es totalmente transparente para el cliente.

COBIT: Control Objectives for Information and related Technology

Codificación: es un procedimiento que consiste en el ordenamiento de datos para su aceptación y ejecución por un sistema automático de cómputo.

Código Fuente: Es un conjunto de líneas de texto que son las instrucciones que debe seguir la computadora para ejecutar dicho programa.

.com: (del inglés ***com****mercial*) es un dominio de internet genérico que forma parte del sistema de dominios de internet.

CONDUSEF: Comisión Nacional para la Protección y Defensa de Usuarios de Servicios Financieros.

Conexión: Ruta de comunicaciones dedicada punto a punto o conmutada.

Concientizar: Acción y efecto de crear conciencia entre la gente acerca de un problema o fenómeno que se juzga importante.

Conficker: También conocido como **Downup Devian**, **Downandup** y **Kido**, es un gusano informático que apareció en octubre de 2008, que ataca el sistema operativo Microsoft Windows.

Confidencialidad: La confidencialidad ha sido definido por la Organización Internacional de Estandarización (ISO) en la norma ISO-17799 como "garantizar que la información es accesible sólo para aquellos autorizados a tener acceso" y es una de las piedras angulares de la seguridad de la información.

Configuración: Es un conjunto de datos que determina el valor de algunas variables de un programa o de un sistema Operativo, estas opciones generalmente son cargadas en su inicio y en algunos casos se deberá reiniciar para poder ver los cambios, ya que el programa no podrá cargarlos mientras se esté ejecutando, si la configuración aún no ha sido definida por el usuario (personalizada), el programa o sistema cargará la configuración por defecto (predeterminada).

Contingencia: Posibilidad de que algo suceda. Lo que puede o no suceder.

Contraseña: Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

Correo electrónico: Sistema para enviar mensajes en Internet. El emisor de un correo electrónico manda los mensajes a un servidor y éste, a su vez, se encarga de enviárselos al servidor del receptor. Para poder ver el correo electrónico es necesario que el receptor se conecte con su servidor.

CPU: *Central Processing Unit* o Unidad Central de Proceso. El "cerebro" de un ordenador; en general, sinónimo de microprocesador. En ocasiones se usa para referirse al toda la caja que contiene la placa base, el micro y las tarjetas de expansión.

Cracker: un *hacker* con intenciones destructivas o delictivas.

Criptografía: Rama del conocimiento que se encarga de la escritura secreta, originada en el deseo humano por mantener confidenciales ciertos temas.

CUDI: Corporación Universitaria para el desarrollo de Internet A.C.

Curiosos: Personas con un alto interés en las nuevas tecnologías, pero no cuentan con la suficiente experiencia para ser considerados como hackers o crackers.

D

Data Center: Se denomina **centro de procesamiento de datos (CPD)** a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización.

Data Diddling: Se refiere a la modificación desautorizada de los datos o al software instalado en un sistema, incluyendo borrado de archivos.

Datagrama: Paquete individual de datos que es enviado a un equipo receptor sin ninguna información que lo relacione con ningún otro posible paquete.

Decodificar: Pasar un texto codificado a un lenguaje que se puede leer directamente.

Delito informático: Delito cometido utilizando un PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.

Deontología: Se refiere a un conjunto ordenado de deberes y obligaciones morales que tienen los profesionales de una determinada materia. La deontología es conocida también bajo el nombre de "Teoría del deber" y junto con la axiología es una de las dos ramas principales de la Ética normativa.

DGESCA: Dirección General de Servicios de Cómputo Académico.

DHCP (Dynamic Host Configuration Protocol): Protocolo destinado a la obtención de una dirección IP para nuestra conexión a Internet de manera aleatoria, en lugar de disponer permanentemente de una única dirección

Digital: Dispositivo o método que utiliza variaciones discretas en el voltaje, la frecuencia, la amplitud, la ubicación, u otros, para cifrar, procesar o transportar señales binarias (0 ó 1) para datos informáticos, sonido, vídeo u otra información.

DNS: Domain Name System

DNS Spoofing: Hace uso de información falsa recibida desde un host que no es autoridad para la información.

Disco duro: Disco magnético de gran capacidad que se utiliza para almacenar datos y programas. En la actualidad los hay de varios Gigabytes. Medio fijo usualmente, pero también los hay removibles.

Disponibilidad: El objetivo de la disponibilidad es garantizar el acceso a un servicio o a los recursos.

Disquete: es un medio o soporte de almacenamiento de datos formado por una pieza circular de material magnético, fina y flexible (de ahí su denominación) encerrada en una cubierta de plástico cuadrada o rectangular.

Dispositivo: En comunicaciones, elemento integral de las redes de comunicación de datos que se caracteriza por manejar flujos de información y que determina la frontera o el punto de demarcación entre la red de datos del Usuario y la red pública de datos.

DNS (Domain Name System): Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP, por ejemplo de: www.asesoriainformatica.com a: 200.57.147.12.

DoS (Denial of Service): Los ataques de denegación de servicio tienen como objetivo saturar los recursos de la víctima, de tal manera que se inhabilitan los servicios brindados por la misma.

DOMINIO: Sistema de gestión de bases de datos, es el rango limitado de valores válidos para un campo. Por ejemplo, un dominio puede estar restringido a caracteres numéricos, como sucede en el caso de los números de teléfono. En redes que utilizan el protocolo TCP/IP, como Internet, un dominio es un grupo de ordenadores conectados. Dentro de un dominio puede haber subdominios. En Internet, los dominios se representan por un código normalmente de tres letras. Entre los más comunes están .edu (institución educativa), .gob (gobierno, hispano), .com (sitio comercial), .mil (sitio militar), .net (proveedora de comunicaciones), .org (organización no lucrativa). Indicadores de zonas geográficas: .mx (de México).

DOS (Disk Operating System): Programa que controla el funcionamiento del ordenador. Es el sistema operativo utilizado en la mayoría de las computadoras personales (PCs) existentes. La más conocida es la desarrollada por Microsoft, denominada MS-DOS.

E

Ebay: Sitio destinado para la subasta de productos a través de Internet.

Eficiencia: Capacidad para realizar o cumplir adecuadamente una función: *la eficiencia en el trabajo.*

EI: Ética informática.

Emisor: Quien emite un mensaje.

Emulador: Programa que permite a un dispositivo realizar una función propia de otro.

Energía eléctrica: Se denomina **energía eléctrica** a la forma de energía la cual resulta de la existencia de una diferencia de potencial entre dos puntos, lo que permite establecer una corriente eléctrica entre ambos (cuando se les coloca en contacto por medio de un conductor eléctrico) para obtener trabajo. La energía eléctrica puede transformarse en muchas otras formas de energía, tales como la energía luminosa o luz, la energía mecánica y la energía térmica.

ENIAC: Electronic Numerical Integrator And Computer.

Encriptación: Proceso de cifrar la información para proteger su uso o visualización no autorizado durante el proceso de transmisión o cuando se guarda en algún medio transportable.

Escaner: Programa que busca virus en la memoria del PC o en los archivos.

Espectro: Gama de frecuencias electromagnéticas de radio utilizada en la transmisión de datos, audio y vídeo.

Ética: Es una rama de la filosofía que abarca el estudio de la moral, la virtud, el deber, la felicidad y el buen vivir.

.exe: De la abreviación del inglés *executable*, que se traduce en *ejecutable.* Es una extensión que se refiere a un archivo ejecutable de código reubicable, es decir, sus direcciones de memoria son relativas.

Exploit: Programa que aprovecha el agujero dejado por un bug / Método concreto de usar un bug para entrar en un sistema.

Facebook: Sitio de redes sociales donde la gente se reúne con las personas que conocen o conocen a nuevas personas.

Falso negativo: Evento que se da como inexistente cuando realmente si existe, por ejemplo, decir que un sistema está limpio de virus cuando realmente está infectado.

Falso positivo: Evento que se da como existente cuando realmente no existe, por ejemplo, decir que un sistema está infectado de virus cuando realmente está limpio

Fibra óptica: Combinación de vidrio y materiales plásticos. A diferencia del cable coaxial y del par trenzado no se apoya en los impulsos eléctricos, sino que transmite por medio de impulsos luminosos. Es el medio físico por medio del cual se pueden conectar varias

computadoras.

Filtro de paquetes: Un filtro de paquetes es un componente de software con la capacidad para examinar las cabeceras de los paquetes que lo atraviesan y de tomar decisiones, según esas cabeceras, sobre el destino de cada uno de los paquetes.

Firewall: Programa o equipo que separa a un equipo, una red local (LAN) o una red global (WAN) en dos o más partes, con propósitos de seguridad, limitando o supervisando los accesos a sus recursos.

Firma digital: Conjunto de datos, en forma electrónica, anexos a otros datos del mismo tipo o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge y que impide la apropiación o daño de su contenido por parte de terceros. Se obtiene cifrando la huella digital de un mensaje con la clave privada del remitente. Garantiza la identidad del firmante y que el texto no se modificó.

Firmware: Indica el tipo de Software almacenado de modo permanente en un ship ROM.

Fraude: La estafa es un delito contra la propiedad o el patrimonio.

Freeware: Política de distribución gratuita de programas. Utilizada para gran parte del software de Internet. En general, estos programas son creados por un estudiante o alguna organización (usualmente una Universidad).

FTP: File Transfer Protocol (Protocolo de transferencia de archivos). Método común de enviar archivos entre computadoras en Internet

Fuga de información: ocurre cuando un sistema diseñado para realizar tareas que no deben ser observadas por un atacante revela parte de esa información debido a errores en los procedimientos de trabajo.

G

Garantizar: Dar garantía de que una cosa va a suceder o realizarse.

Gateway: Programa o equipo que se encarga de traducir la información contenida en dos protocolos diferentes.

Gbps: 1.024 MB por segundo.

Gestión: Dirección, administración de una empresa, negocio, etc.

Google: Es un motor de búsqueda reconocido y el más grande del mundo. Aparte de eso tiene muchos programas útiles, aplicaciones web y herramientas. Las más importantes para

propósitos de posicionamiento web son el Google Sitemap, y los programas de publicidad Adsense y Adwords.

GPS (Sistema de Posicionamiento Global): Sistema de navegación por satélite con cobertura global y continua que ofrece de forma rápida y temporalmente bastante precisa una posición geográfica de un elemento.

Gusano: Programa informático que se reproduce así mismo copiándose una y otra vez de sistema en sistema y que usa recursos de los sistemas atacados.

H

Hacker: Nombre que se da a un usuario con avanzados conocimientos y que dedica mucho tiempo a trabajar con los ordenadores. Originalmente se utilizaba el término para designar a una persona que escribe programas informáticos, troceando (hacking) el código digital. La palabra hacker se utiliza generalmente para designar a las personas que rompen los sistemas de seguridad

Hardware: Soporte físico o material. Partes tangibles de cómputo.

HIDS (Sistema de detección de intrusos en un Host): Busca detectar anomalías que indican un riesgo potencial, revisando las actividades en la máquina (host). Puede tomar medidas protectoras

Hipertexto: Describe un tipo de funcionalidad de exploración en línea interactiva. Los vínculos (direcciones URL) incrustados en palabras o frases permiten al usuario escoger un texto concreto para que se muestre inmediatamente la información relacionada y el material multimedia asociado

Hipervínculo: Conexiones entre una información y otra dentro de un documento HTML.

Honeynets: Los Honeynet son un tipo especial de Honeypots de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes. Se usan equipos reales con sistemas operativos reales y corriendo aplicaciones reales.

Honeypot: Un servidor diseñado para ser atacado y que actúa como señuelo para hackers los cuales piensan que se conectan a un verdadero sistema informático y actúan sobre él, permitiendo así a su propietario monitorizar la actividad del "pirata" con distintos fines: estudiar su comportamiento, fijar los puntos débiles de su red, entre otros.

Host: Computadora en una red. Antes se denominaba con el término "nodo" que se utiliza en el lenguaje de definición de documentos. Muchas veces se usa como sinónimo de servidor.

Hotmail: Es el más popular correo electrónico de sitio web y cuenta con millones de usuarios a nivel mundial. Recientemente fue comprado por MSN Networks, empresa miembro del grupo Microsoft.

HTTP (Hipertext Transfer Protocol): Protocolo de transferencia de hipertexto. Conjunto de estándares que permite a los usuarios de la Web intercambiar información. Método que se utiliza para transferir documentos desde el sistema donde se almacenan las páginas hasta los usuarios individuales

HTTPS (Protocolo seguro de transferencia de hipertexto): Es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

Hub: Concentrador. Dispositivo que se utiliza típicamente en topología en estrella como punto central de una red, donde por ende confluyen todos los enlaces de los diferentes dispositivos de la red.

I

IBM (International Business Machines): Conocida coloquialmente como **el Gigante Azul**) es una empresa multinacional que fabrica y comercializa herramientas, programas y servicios relacionados con la informática.

ICMP: El **Protocolo de Mensajes de Control de Internet** o **ICMP** (por sus siglas de ***I**nternet **C**ontrol **M**essage **P**rotocol*) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

IDS (Sistema de Detección de Intrusos): En sus siglas en inglés *Intrusion Detection System*, es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

IEC: Internacional Electrotechnical Comission.

IEEE (Institute of Electrical and Electronic Engineers): Instituto de Ingenieros Eléctricos y Electrónicos.

IEEE 802.11: Familia de estándares desarrollados por la IEEE para tecnologías de red inalámbricas (wireless). Permite la conexión de dispositivos móviles (lap-top, PDA, teléfonos celulares a una red cableada, por medio de un Punto de Acceso (Access Point). La conexión se realiza a través de ondas de Radio Frecuencia. Originalmente ofrecía una velocidad de transmisión de 1 o 2 Mbps en la banda de frecuencia de 2.4 GHz. Se le conoce popularmente como WIFI. Tiene un área de cobertura aproximada de 100 ms.

IEEE 802.11a: Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de 5 GHz. Utiliza la tecnología OFDM (Orthogonal Frecuency División Multiplexing. Esta banda de 5GHz no se pudo utilizar en muchos países, al comienzo, por estar asignada a las fuerzas y organismos de seguridad.
IEEE 802.11b: Estándar de conexión wireless que suministra una velocidad de transmisión de 11 Mbps en una banda de 2.4 GHz. Utiliza la tecnología DSSS (Direct Sequencing Spread). La mayoría de los equipos utilizados en la actualidad son de esta tecnología. Fue ratificado en 1999. No es compatible con el 802.11a pues funciona en otra banda de frecuencia.

IEEE 802.11e: Estándar en elaboración desde Junio de 2003, destinado a mejorar la calidad de servicio en Wi-Fi (QoS – Quality of Service). Es de suma importancia para la transmisión de voz y video.

IEEE 802.11g: Estándar de conexión wireless que suministra una velocidad de transmisión de 54 Mbps en una banda de frecuencia de 2.4 GHz. Se basa en la tecnología OFDM, al igual que el estándar 802.11a. Fue ratificado en Junio de 2003. Una de sus ventajas es la compatibilidad con el estándar 802.11b.

IEEE 802.11i: Estándar de seguridad para redes wifi aprobado a mediados de 2004. En el se define al protocolo de encriptación WPA2 basado en el algoritmo AES.

IEEE 802.11n: Estándar en elaboración desde Enero 2004. Tiene como objetivo conseguir mayores velocidades de transmisión para Wi-Fi. Estas serán superiores a 100 Mbps. Hay 2 propuestas distintas. En 2006 se aprobará una de las dos. La de TGn Sync o la WWiSE.

IEEE 802.16: Estándar de transmisión wireless conocido como WIMAX (Worldwide Interoperability for Microwave Access). Es compatible con WIFI. Se originó en Abril de 2002 con la finalidad de cubrir inalámbricamente distancias de hasta 50 Km. La tecnología permite alcanzar velocidades de transmisión de hasta 70 Mbits en una banda de frecuencias entre 10 GHz y 66 GHz. La interoperatividad es certificada por el WIMAX FORUM.

IEEE 802.16d Estándar de transmisión wireless (WIMAX*) que suministra una velocidad de entre 300 K y 2 Mbps en una banda de frecuencia de 2GHz a 11GHz. Ratificado a finales de 2004. Se utiliza para el cubrimiento de la “primer milla”.

IEEE 802.1x: Estándar de seguridad para redes inalámbricas y cableadas. Se apoya en el protocolo EAP y establece la necesidad de autenticar y autorizar a cada usuario que se conecte a una red.

IMAP (Internet Message Access Protocol): Es protocolo de red de acceso a mensajes electrónicos almacenados en un servidor.

IMCO: Instituto Mexicano para la Competitividad.

Implantación: Establecimiento de algo nuevo en un lugar, generalmente que ya existía o funcionaba con continuidad en otro sitio o en otro tiempo: *la implantación de cajeros automáticos.*

Implementación: es la realización de una aplicación, o la ejecución de un plan, idea, modelo científico, diseño, especificación, estándar, algoritmo o política.
Incidente: Lo que sobreviene en el curso de un asunto y tiene cierta relación con él. Acontecimiento imprevisto.

Información: Es un conjunto organizado de datos **procesados**, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Informática: Es el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.

Ingeniería: conjunto de conocimientos y técnicas científicas aplicadas a la invención, perfeccionamiento y utilización de la técnica industrial en todos sus diversos aspectos incluyendo la resolución u optimización de problemas que afectan directamente a los seres humanos en su actividad cotidiana.

Ingeniería Social: Significa engañar a alguien para que revele información útil para los atacantes, tales como una contraseña, por correo electrónico, por teléfono o personalmente.

Ingeniería Social Inversa: Es generar una situación inversa a la original en la ingeniería social. El atacante lo que hace es brindar una ayuda a los usuarios (posibles victimas), ellos llaman si se presenta alguna anomalía en el sistema, es aquí donde el delincuente aprovecha esa oportunidad para pedir información necesaria para solucionar el problema del usuario y el del atacante por supuesto (la forma de acceder al sistema).

Inserción: Inclusión o introducción de una cosa en otra.

Instalación eléctrica: Es uno o varios circuitos eléctricos destinados a un uso específico y que cuentan con los equipos necesarios para asegurar el correcto funcionamiento de ellos y los aparatos eléctricos conectados a los mismos

Inteligencia Artificial: Se denomina Inteligencia Artificial a la rama de las ciencias de la computación dedicada al desarrollo de agentes racionales no vivos.

Integridad: La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).

Interfaz Hardware: Punto de contacto entre dos sistemas o módulos de un sistema.

Interfaz Software: Parte de un programa que sirve para comunicarse con otro programa, con una parte del hardware o con el usuario.

Internauta: Persona que navega por Internet.

Internet: (**inter:** internacional, **net:** red). Red mundial que conecta entre sí a computadoras del mundo mediante el protocolo IP y proporciona diversos servicios de intercambio de información. En su primera etapa la conexión de las computadoras fue a través de la red telefónica existente. Actualmente se desarrollan conexiones por medio de fibra óptica y vía inalámbrica.
Internet2: La nueva versión de Internet que permite la transmisión de datos a alta velocidad, mayor seguridad y mayor confiabilidad.

Internet World Stast: Estadísticas del mundo en Internet.

InterNIC: Internet Network Information Center.

Interoperabilidad: Es la capacidad de dos o más componentes o sistemas de intercambio de información de poder utilizar la información que se ha intercambiado.

Intranet (Red interna): Red que utiliza los protocolos de Internet pero que es de uso interno, por ejemplo, la red corporativa de una empresa. Puede exponer parcialmente información al exterior vía Internet.

Intruso remunerado: Personas con gran experiencia en seguridad y conocimiento amplio de los sistemas. Son pagados por una tercera persona para robar secretos o dañar la imagen de la empresa.

IP: DIRECCIÓN IP. Dirección de 32 bits del protocolo Internet asignada a un ordenador conectado a Internet. La dirección IP tiene un componente del propio ordenador y un componente de la red. Este número tiene el formato de cuatro grupos de hasta tres dígitos, separados por un punto, por ejemplo 172.16.253.90.

IPN: Instituto Politécnico Nacional.

IPSec: Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtuales (VPNs), soporta dos modos de encriptación: Transporte y Túnel. El primero sólo encripta la parte relativa a los de datos (payload) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, encripta todo.

IP Spoofing: Hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

IPV6: El protocolo Internet versión 6 es una nueva versión de IP (*Internet Protocol*), definida en el RFC 2460 y diseñada para reemplazar a la versión 4 (IPv4) RFC 791, que actualmente esta implementado en la gran mayoría de dispositivos que acceden a Internet.

Iphone: Teléfono inteligente multimedia con conexión a Internet, pantalla táctil capacitiva (con soporte multitáctil) y una interfaz de hardware minimalista de la compañía Apple Inc.

IRC: Internet Realy Chat.

ISDN: (Red digital de servicios integrados). Juego de normas de la transmisión a gran velocidad de información simultánea de voz, datos e información a través de menos canales de los que serían necesarios de otro modo, mediante el uso de la señalización fuera de banda.

ISO (International Standard Organization): Fundada en 1947 reúne asociaciones de muchos países y su objetivo es establecer los estándares internacionales, incluidos para la comunicación de datos.

ISOC: Internet Society

ISP Internet Service Provider: Organización o empresa que establece la conexión entre los usuarios e Internet. Generalmente, los ISP ofrecen servicios de conexión, correo electrónico, hospedaje de páginas Web y el software de navegación por la Web. El ISP ofrece un número de teléfono, por lo general local, para que los usuarios se conecten a su servidor y puedan acceder a la Red mundial.

ITU: Unión Internacional de Comunicaciones.

K

Kbps: Kilobites por segundos, kbit/s. Un kbps equivale a 1000 bits por segundo. Generalmente usado para medir velocidades de conexión o transferencias en una red.

Kerberos: Kerberos es un protocolo de seguridad creado por MIT que usa una criptografía de claves simétricas para validar usuarios con los servicios de red (evitando así tener que enviar contraseñas a través de la red). Al validar los usuarios para los servicios de la red por medio de Kerberos, se frustran los intentos de usuarios no autorizados que intentan interceptar contraseñas en la red.

Keylogger: Un registrador de teclas ("keylogger") es un programa de computadora que registra cada tecla que un usuario presiona en un teclado y guarda esta información en un archivo o la transfiere a través de Internet hacia un servidor remoto predeterminado.

L

LAN (Local Area Network): Conjunto de ordenadores conectados entre sí y dentro de la misma área física. Facilita poder disponer de los recursos de varios ordenadores dentro de un grupo de trabajo.

Linux: GNU/Linux es uno de los términos empleados para referirse a la combinación del núcleo o *kernel* libre similar a Unix denominado **Linux**, que es usado con herramientas de sistema GNU

Login: Clave de acceso que se le asigna a un usuario para que pueda utilizar los recursos de una red o computadora. El login define al usuario y lo identifica dentro de una red junto con la dirección electrónica de la computadora que utiliza.

M

MAC (Dirección de Control de Acceso a Medios): Dirección hardware de 6 bytes (48 bits) única que identifica únicamente cada nodo (tarjeta) de una red y se representa en notación hexadecimal. En redes IEEE 802, la capa Data Link Control (DLC) del Modelo de Referencia OSI se divide en dos sub-capas: Logical Link Control (LLC) y Media Access Control (MAC), la cual se conecta directamente con el medio de red. Consecuentemente, cada tipo de medio de red diferente requiere una capa MAC diferente. En redes que no siguen los estándares IEEE 802 pero sí el modelo OSI , la dirección del nodo se denomina Data Link control (DLC) address.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Malware: Programa o parte de un programa que tiene un efecto malicioso en la seguridad de los sistemas. Este término engloba muchas definiciones como virus, gusanos, troyanos, spyware, etc.

MAN Red de Área Metropolitana: Metropolitan area network en inglés. Es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo.

Mbps: Megabits por segundo, Mbit/s. Un mbps equivale a un millón de bits (o 1000 kbit) transferidos por segundo. Suele utilizarse para medir la velocidad de una conexión como la de Internet o para medir calidad de videos. Generalmente se le llama "mega", pero no debe confundirse con la unidad de almacenamiento que también suele llamársele "mega" y equivale a 1024 kilobytes.

Memorias de Almacenamiento: se refiere a los componentes de una computadora, dispositivo y medios de almacenamiento que retienen datos informáticos durante algún intervalo de tiempo.

Mensajería instantánea: La Mensajería Instantánea es un punto intermedio entre los sistemas de chat y los mensajes de correo electrónico, las herramientas de mensajería instantánea, son programas regularmente gratuitos y versátiles, residen en el escritorio y, mientras hay una conexión a Internet, siempre están activos.

Mesa de ayuda: La Mesa de Ayuda es un servicio creado para facilitar la comunicación e interacción con el ciudadano. A través de ella se brindan respuestas a consultas sobre temas impositivos, previsionales y aduaneros; ya sea sobre la normativa, aplicativos o servicios web.

Messenger: Programa de mensajería instantánea.

Microsoft: Casa desarrolladora de software, creadora de sistemas operativos como MS-DOS y Windows, así como de aplicaciones informáticas de todo tipo.
Mitigar: Reducir o disminuir algo.

MODEM: Dispositivo que adapta las señales digitales para su transmisión a través de una línea analógica, normalmente telefónica.

Modificación: Alteración de una cosa que no afecta a sus características principales.

Monitoreo: Monitorizar, observar el curso de uno o varios parámetros para detectar posibles anomalías.

Mouse: Periférico de ordenador utilizado para señalar elementos en la pantalla

Mozilla firefox: Es un navegador web libre y de código abierto, y que cualquier usuario puede ayudar a su desarrollo.

MPEG (Moving Pictures Expert Group): Formato estándar de almacenamiento para comprimir vídeo de imágenes en movimiento. Utiliza compresión con perdidas, alcanzando niveles de reducción de tamaño muy altos.

MS-DOS: Microsoft Disk Operating System. (Sistema Operativo en Disco de Microsoft). Sistema operativo empleado en los primeros IBM PC y que ha estado en la base de todos los sistemas operativos de Microsoft hasta la aparición de Windows NT.

MULTICASTING: Técnica de transmisión de datos a través de Internet en la que se envían paquetes desde un punto a varios simultáneamente.

Multimedia: Sistemas informáticos que integran audio, vídeo y datos. También se emplea la acepción para definir la información digitalizada que combina texto, gráficos, imagen fija y en movimiento, así como sonido.

N

Navegador: Aplicación para visualizar documentos web y navegar por internet. Término aplicado a los programas que permiten acceder al servicio WWW. Los navegadores gráficos pueden mostrar imágenes y texto y permiten desplazarse de una página a otra utilizando el ratón.

Netscape: Programa cliente de WWW que permite que el viaje por Internet sea más divertido.

NIDS (Sistema de detección de intrusos en una Red): Busca detectar anomalías que inicien un riesgo potencial, tales como ataques de denegación de servicio, escaneadores de puertos o intentos de entrar en un ordenador, analizando el tráfico en la red en tiempo real.

No repudio: Proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación.

Nodo: Su definición original es la de punto donde convergen dos líneas. En informática, el término se refiere muchas veces a una máquina conectada a Internet, aunque lo normal es que se hable de un punto de confluencia en una red.

Norma: Regla de obligado cumplimiento.

O

OCDE: Organización para la Cooperación y el Desarrollo Económico.

OCTAVE: Operationally Critical Threats Assets and Vulnerability Evaluation.

Online: Algo o alguien que se encuentra en Internet.

Optimizar: Planificar una actividad para obtener los mejores resultados: *han hecho cambios de personal con el fin de optimizar los rendimientos.*

OSI (Open Systems Interconnection): Interconexión de Sistemas Abiertos. Modelo de referencia de interconexión de sistemas abiertos propuesto por la organización de normalización ISO. Divide las tareas de la red en siete niveles.

P

Paquete: Conjunto limitado de datos unidos.

Pasword: Contraseña asociada a un login para poder acceder a un sistema o recurso.

PDA (Personal Digital Assistant): Asistente Personal Digital. Dispositivo de reducidas dimensiones y portátil que se utiliza para controlar tareas habituales del usuario, como la gestión de una agenda, un listado de direcciones o lista de cosas por hacer. También se pueden emplear para enviar faxes y mensajes de correo electrónico.

Permisible: Que puede ser permitido: *ese tipo de travesuras solo es permisible en los niños.*

Personal interno: Amenazas provenientes del personal del propio sistema informático.

PHARMING: Acceso ilegal al servidor DNS local. Su principal objetivo es manipular las direcciones DNS (Domain Name Server) sustituyendo las páginas originales por páginas falsas, con el objetivo de recabar datos confidenciales de los visitantes

Phishing: Técnica de ingeniería social usada para engañar a los usuarios con el fin de obtener sus contraseñas, nombres de usuario y otro tipo de información personal.

Phreakers: Individuo que lanza ataques a sistemas telefónicos privados.

Ping Packet INternet Groper: Rastreador de Paquetes Internet. Utilidad del protocolo TCP/IP que permite comprobar si un servidor o equipo está disponible. Envía paquetes de control para comprobar si el servidor o el equipo esta activo y los devuelve.

Políticas de Seguridad: Conjunto de requisitos definidos por los responsables directos o indirectos de un sistema, indica en términos generales lo que está y lo que no está permitido.

POP: Conexión de acceso telefónico de los proveedores de servicios de Internet para usuarios de módem, que se utiliza principalmente para describir conexiones locales, de forma que los usuarios no tengan que hacer llamadas de larga distancia. Por ejemplo, un determinado ISP puede tener su base en San José, pero tener "POP" en Los Ángeles y Nueva York.

Programación: Acción que consiste en hacer una planificación ordenada de las distintas partes o actividades que componen una cosa que se va a realizar: *programación de las fiestas.*

Prohibitivo: Que prohíbe o sirve para prohibir: *una ley prohibitiva.*

Proteger: Hacer que una persona o cosa no sufra daño o no esté en peligro: *esta crema protege del sol.*

Protocolo: Conjunto de reglas y normas que determinan cómo se realiza un intercambio de datos, asegurando que los datos recibidos son idénticos a los datos enviados.

Proxy: También conocido como servidor caché, se trata de una máquina conectada al servidor de acceso a WWW de un proveedor de acceso y en la que se va almacenando toda la información que los usuarios reciben de la web. De esta forma, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información que se almacena en el servidor en lugar del servidor real.

Puerto: Dispositivo físico o lógico que forma parte de la infraestructura de una red o de un equipo y que funge como interface entre el equipo de datos del Usuario y la red o el equipo y sus dispositivos.

R

Recurso: Ayuda o medio al que se puede recurrir para conseguir un fin o satisfacer una necesidad: *siempre tiene algún recurso ingenioso para salir con buen pie de las situaciones complicadas; el agua es un recurso escaso y fundamental para la vida*
Red: Sistema de elementos interrelacionados que se conectan mediante un vínculo dedicado o conmutado para proporcionar una comunicación local o remota (de voz, vídeo, datos, entre otros) y facilitar el intercambio de información entre usuarios con intereses comunes.

Red Ad hoc: Es una red inalámbrica descentralizada. La red es ad hoc porque cada nodo está preparado para reenviar datos a los demás y la decisión sobre qué nodos reenvían los datos se toma de forma dinámica en función de la conectividad de la red.

Red inalámbrica: Una **red inalámbrica** es, como su nombre lo indica, una red en la que dos o más terminales (por ejemplo, ordenadores portátiles, agendas electrónicas, entre otros) se pueden comunicar sin la necesidad de una conexión por cable.

Red local: Una red local es la interconexión de varios ordenadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros.

Redes de computadoras: Conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que compartan información (archivos), recursos (CD-ROM, impresoras, entre otros), servicios (acceso a internet, e-mail, chat, juegos).

Redes sociales: Redes en cuya estructura los nodos individuales son personas que mantienen relaciones, tales como amistad, intereses comunes o fines comerciales.

Repetidor: Equipo que incluye esencialmente uno o varios amplificadores o regeneradores -o ambos- y dispositivos asociados; está insertado en un punto de un medio de transmisión con objeto de restituir a su estado de partida las señales atenuadas, debilitadas o deformadas en el curso de la propagación.

Reputación: Opinión que se tiene sobre alguien.

Resguardarse: Prevenirse contra un daño.

Respaldo: Protección o apoyo.

Robo: Apropiación indebida de algo ajeno, contra la voluntad de su poseedor, especialmente si se hace con violencia

Router: Dispositivo que une entre sí dos redes, de forma que la información que no va dirigida a la otra red, no pasa a ella.

S

Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo.

Seguridad: Esta palabra viene del latín *seguritas*, se refiere a la cualidad de seguro, es decir, aquello que está exento de peligro, daño o riesgo. Algo seguro es algo cierto. La seguridad por lo tanto es una certeza.

Seguridad Informática: Disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático.

Señal: Cambio de estado orientado a eventos (p. ej. un tono, cambio de frecuencia, valor binario, alarma, mensaje, entre otros).

Servidor: En una red, es un ordenador que proporciona servicios a otros equipos (estaciones).

Sesión: Es la duración de una conexión empleando una capa de sesión de un protocolo de red, o la duración de una conexión entre un usuario (el agente) y un servidor, generalmente involucrando el intercambio de múltiples paquetes de datos entre la computadora del usuario y el servidor.

SGBD: Sistema de Gestión de Bases de Datos.

Shareware: Se denomina a una modalidad de distribución de software, tanto videojuegos como programas utilitarios en las que el usuario puede evaluar de forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de las formas de uso con restricciones en las capacidades finales.

SHELL: Intérprete de comando de un sistema operativo. Se encarga de tomar las órdenes del usuario y hacer que el resto del sistema operativo las ejecute.

Sistema: Conjunto ordenado de normas y procedimientos que regula el funcionamiento de una colectividad: *el sistema de gobierno que tenemos en España es la democracia; el sistema monetario internacional regula los cambios de moneda para que sean estables y puedan efectuarse correctamente las transacciones comerciales*

SMTP (Simple Mail Transfer Protocol): (Protocolo de Transferencia Simple de Correo). Protocolo usado para gestionar el correo electrónico a través de Internet. Define el formato que deben tener los mensajes y cómo deben ser transferidos.

Spam: Correo electrónico no solicitado, por lo común de carácter comercial, enviado de forma indiscriminada a varias listas de correo, individuos o grupos de noticias (correo electrónico basura).

Spyware: Un software espía es un software que puede parecerse al adware, pero se utiliza para controlar el uso de la computadora sin el conocimiento o consentimiento del usuario. Los software espía pueden grabar la secuencia de pulsación de teclas, el historial de navegación, contraseñas y cualquier otra información confidencial y privada, y enviar estos datos a un tercero vía Internet.

Sistema: Conjunto de elementos que, ordenadamente relacionadas entre sí, contribuyen a determinado objeto

Sistemas de comunicación: es un conjunto de recursos y esfuerzos con el objetivo de dar apoyo a todas las áreas y procesos de la organización, con acciones para facilitar el cumplimiento del plan estratégico, alinear los procesos y propiciar un ambiente positivo.

Sistema de información: Es un conjunto organizado de elementos, que pueden ser personas, datos, actividades o recursos materiales en general. Estos elementos interactúan entre sí para procesar información y distribuirla de manera adecuada en función de los objetivos de una organización.

Sistema operativo: Capa de enlace entre Hardware/Software, que permite a los programas abstraerse del soporte físico y verlo como una serie de recursos con estructura similar a la de los programas. Ejemplos: Linux, Unix, Windows, OS, etc.

SMTP: Protocolo Simple de Transferencia de Correo.

Sniffer: Programa de captura de las tramas de red.

Socket: Designa un concepto abstracto por el cual dos programas (posiblemente situados en computadoras distintas) pueden intercambiar cualquier flujo de datos, generalmente de manera fiable y ordenada. Un *socket* queda definido por una dirección IP, un protocolo de transporte y un número de puerto.

Software: Conjunto de programas para el tratamiento de la información. Elemento intangible de un equipo de cómputo.

SPOOFING: Creación de tramas TCP/IP con la ayuda de una dirección IP falsa. El generador del spoofing trata de simular la identidad de otra máquina para conseguir el acceso a los recursos de una red.

Spyware: Cualquier tipo de software que utiliza la conexión a internet del usuario para enviar información sobre su actividad, misma que es utilizada por las empresas publicitarias para enviar propaganda de acuerdo a su actividad en la red.

SQL (Structured query language): Lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en éstas.

SSID (Service Set IDentifier): Es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos pero el estándar no lo especifica así que puede consistir en cualquier carácter. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Symantec: Corporación internacional que desarrolla y comercializa software para computadoras.

T

TCP/IP Transfer Control Protocol/Internet Protocol: Protocolo de control de transmisiones / Protocolo Internet. Protocolo estándar de comunicaciones en red y transporte del modelo OSI, utilizado para conectar sistemas informáticos a través de Internet.

Tecnología: Conjunto de los conocimientos, instrumentos y métodos técnicos empleados en un sector profesional: tecnología de la información.

Tecnologías de Información: Aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información.

Telecomunicaciones: Es una técnica que consiste en la transmisión de un mensaje desde un punto hacia otro, usualmente con la característica adiciona de ser bidireccional.

Telefonía Móvil: Servicio de telecomunicaciones que mediante una red de antenas situadas en estaciones base permite recibir y realizar llamadas desde terminales móviles por medio de ondas electromagnéticas de radiofrecuencia (señales de mayor frecuencia que las utilizadas en radiotelevisión, pero con una menor potencia)

Telemedicina: Algunas actividades de la medicina, tales como diagnóstico remoto o transmisión de imágenes radiológicas, realizadas mediante la utilización de redes de telecomunicaciones.

TELMEX: Teléfonos de México.

TELNET: Servicio de acceso remoto a Internet. Dicho servicio permite a los usuarios interactuar, desde un lugar determinado, con un sistema de tiempo compartido (como UNIX) distante, como si la terminal del usuario estuviera conectada directamente al servidor de la red.

Terrorismo: Violencia aplicada con el objetivo de aterrorizar a grupos de personas indiscriminadamente o dirigida a un grupo específico, como son los turistas.

TKIP (Temporal Key Integrity Protocol): También llamado hashing de clave WEP WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente.

Topología: Se refiere a cómo se establece y se cablea físicamente una red. La elección de la topología afectará la facilidad de la instalación, el costo del cable y la confiabilidad de la red. Existen tres topologías principales de red anillo, bus y estrella.

Transmisión: Envío y recepción de datos entre los componentes internos y externos del equipo informático.

Trashing: Consiste en rastrear en las papeleras en busca de información, contraseñas o directorios.

Troyano: Programa informático cuya ejecución tiene unos efectos imprevistos y, generalmente, insospechados para el usuario infectado. No se les puede denominar virus porque no se replican.

Twitter: Nueva forma de comunicarse en internet. Servicio de micro-blog que permite a sus usuarios enviar y leer las actualizaciones de los otros usuarios (conocidos como "tweets").

U

UDP (User Datagram Protocol): Protocolo de servicios de internet. Se utiliza cuando es necesario transmitir voz o vídeo, y resulta más importante transmitir con velocidades que garanticen la correcta recepción.

UNIVAC: Universal Automatic Computer (Computadora Automática Universal)

UNIX: Sistema operativo multitarea y multiusuario de gran importancia en el desarrollo y evolución de Internet.

USENET (USEer NETwork): Red de carácter público compuesta por un gran número de grupos de noticias y organizada temáticamente

Usuario: Persona que utiliza o trabaja con algún objeto o que es destinataria de algún servicio público, privado, empresarial o profesional.

V

Ventana Emergente: El término anglosajón **pop-up** (en español: **ventana emergente**) denota un elemento emergente que se utiliza generalmente dentro de terminología **Web.** El término denomina a las ventanas que emergen automáticamente (generalmente sin que el usuario lo solicite) mientras se accede a ciertas páginas web. A menudo, las ventanas emergentes se utilizan con el objeto de mostrar un aviso publicitario de manera intrusiva.

Vínculo: Elemento de un documento electrónico que hace referencia a otro recurso, por ejemplo, otro documento o un punto específico del mismo o de otro documento.

Virus: Programa informático que se reproduce a si mismo, indeseable y potencialmente peligroso, que altera el funcionamiento de los ordenadores.

Virtual: Término utilizado con asiduidad en la red, hace referencia a algo que no tiene existencia física o real, solo aparente.

VPN (Virtual Private Network): Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Por ejemplo, los datos se pueden transmitir de forma segura entre dos sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de área local (LAN).

Vulnerabilidad: Capacidad de sufrir un daño.

W

WAP (Wireless access Protocol): Protocolo de acceso inalámbrico. Especificación que permite la comunicación en red a través de un medio inalámbrico.

Web: Nombre coloquial con que se nombra a la World Wide Web. Sistema de comunicación y de publicación que fue diseñado para distribuir información a través de redes de computadoras en una modalidad llamada **hipertexto**.

Web 2.0: La Web 2.0 es la representación de la evolución de las aplicaciones tradicionales hacia aplicaciones web enfocadas al usuario final. El Web 2.0 es una actitud y no precisamente una tecnología.

Web 3.0: E una extensión del **World Wide Web** en el que se puede expresar no sólo lenguaje natural, también se puede utilizar un lenguaje que se puede entender, interpretar utilizar por agentes software, permitiendo de este modo encontrar, compartir e integrar la información más fácilmente.

WDS: Sistema de distribución inalámbrico (WDS por sus siglas en inglés) es un sistema que permite la interconexión inalámbrica de puntos de acceso en una red IEEE 802.11.

WEP: Protocolo para la transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad.

WiFi: Abreviatura de Wireless Fidelity. Nombre “comercial” con el que se conocen a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica. En lenguaje popular: Redes wifi.

WPA: Acceso wi-fi. Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

WPA2 (Wireless Application Protocol): Protocolo de seguridad para redes wifi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Puntos de Acceso de última generación.

Windows: Sistema operativo de Microsoft, que opera en un entorno gráfico.

WWW (World Wide Web): Sistema de información global desarrollado en 1990 por Robert Cailliau y Tim Berners.

Y

YAHOO: Yet Another Hierarchical Officious Oracle.

Youtube: Sito web en el cual los usuarios pueden subir y compartir vídeos.

Z

Zombie: Denominación que se asigna a computadoras tras haber sido infectadas por algún tipo de malware.

Bibliografía

Capítulo 1
Antecedentes de la Seguridad Informática a Nivel Nacional

http://www.cudi.edu.mx/
http://www.accessmylibrary.com/coms2/summary_0286-3146125_ITM
http://www.diarioti.com/noticias/2001/feb2001/15194007.htm
http://www.accessmylibrary.com/coms2/summary_0286-4084872_ITM
http://www2.eluniversal.com.mx/pls/impreso/noticia.html?id_nota=46842&tabla=finanzas
http://www.elsiglodetorreon.com.mx/noticia/15515.alertan-sobre-los-riesgos-de-utilizar-interne.html
http://www.eluniversal.com.mx/notas/348772.html
http://www.elsiglodetorreon.com.mx/noticia/283743.es-lento-el-modem-de-mexico.html
http://www.informador.com.mx/tecnologia/2008/2071/6/ciudades-digitales-y-tecnologia-3g-aceleran-uso-de-internet-en-mexico.htm
http://www.informador.com.mx/tecnologia/2008/37346/1/usuarios-de-internet-en-mexico-crecieron-en-un-341-en-ultimos-ocho-anos.htm
http://www.informador.com.mx/tecnologia/2009/125960/6/impulsan-evolucion-de-internet-en-mexico.htm
http://www.informador.com.mx/economia/2009/93322/6/sin-estrategia-de-seguridad-informatica-80-de-empresas-mexicanas.htm
http://www.cronica.com.mx/nota.php?id_nota=266546
http://www.rumbodemexico.com.mx/macnews-core00005n/notes/?id=215530
http://www.cronica.com.mx/nota.php?idc=225181
http://www.nacion.com/ln_ee/2009/enero/20/aldea1845333.html
http://www.eluniversal.com.mx/articulos/53445.html
http://www.belt.es/expertos/HOME2_experto.asp?id=4021
http://www.jfs.com.mx/e2008.htm
http://www.tudiscovery.com/internet/interactivo.shtml

Capítulo 2
Principales Amenazas

http://www.arcert.gov.ar/politica/versionimpresa.htm
http://pisuerga.inf.ubu.es/~jmsaiz/Cursos/Ses8.pdf
http://www.scribd.com/doc/19397003/Tipos-de-Ataques-informaticos
http://cert.inteco.es/cert/Notas_Actualidad/Informe_Amenazas_informaticas_primer_semestre2009;jsessionid=201D637CFD652A2B66A54AB4CAA04ACE?postAction=getLatestInfo
http://www.segu-info.com.ar/amenazashumanas/curiosos.htm
http://www.segu-info.com.ar/amenazashumanas/interno.htm
http://www.scribd.com/doc/19397003/Tipos-de-Ataques-informaticos
http://www.cisco.com/web/ES/about/press/2009/cisco-noticias-09-07-21.html
https://community.mcafee.com/docs/DOC-1666
http://www.bsecure.com.mx/en-linea/amenazas-mas-peligrosas-en-20-anos/
http://www.cert.org.mx/estadisticas.dsc#2008

Seguridad Informática

http://es.kioskea.net/contents/secu/secuintro.php3
http://www.segu-info.com.ar
http://www.pandasoftware.es/virus_info/
http://www.segu-info.com.ar/fisica/seguridadfisica.htm
http://antares.itmorelia.edu.mx/~jcolivar/courses/dr08/dr_seguridad.ppt#329,49,Referencias

Capítulo 3
Índice de Competitividad

http://www.offnews.info/downloads/europa7.pdf
http://www.cdi.org.pe/IGC_2005_2006.htm
http://economy.blogs.ie.edu/archives/2008/10/indice_de_compe_1.php
http://72.52.156.225/Estudio.aspx?Estudio=indice-competitividad
http://revistafortuna.com.mx/contenido/2010/07/15/seguridad-informatica-inversion-para-el-futuro/

Capítulo 4
Aula Digital

http://www.educacion.df.gob.mx/index.php?option=com_content&task=view&id=1015
http://webcache.googleusercontent.com/search?q=cache:tDqlWul8QGAJ:www.ccat.com.ar/files/Carrera%2520ESP%2520SEG%2520CCAT%25202010.doc+PR%C3%81CTICAS+DE+LABORATORIO+DE+SEGURIDAD+INFORM%C3%81TICA&cd=4&hl=es&ct=clnk&gl=mx

Criptografía

http://www.seguridadenlared.org/es/index25esp.html
http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VII_JornadaSeguridad/VIIJNSI_ACarvajal.pdf

Colegio de Ciencias y Humanidades

http://www.cch.unam.mx/principal/plandeestudios

Escuela Nacional Preparatoria

http://www.planeacion.unam.mx/Memoria/2000/pdf/enp.pdf

Modelo Educativo de Seguridad Informática

http://www.pucp.edu.pe/content/pagina15.php?pID=962&pIDSeccionWeb=4&pIDReferencial=
http://www.efdeportes.com/efd155/la-preparacion-para-la-seguridad-informatica.htm

Facultades

http://www.arq.unam.mx/computo/computo.html
http://www.derecho.unam.mx/web2/modules.php?name=academicos_computo
http://www.fca.unam.mx/cursos_extracurriculares_de_computo.php
http://www.politicas.unam.mx/informatica/apoyamos.pdf
http://132.248.45.5/cife/index.htm
http://www.quimica.unam.mx/IMG/pdf/CI.pdf
http://www.trabajosocial.unam.mx/computo11.html
http://www.filos.unam.mx/computo
http://www.fmvz.unam.mx/fmvz/computo/laborato.html
http://www.facmed.unam.mx/plan/PEFMUNAM.pdf
http://www.derecho.unam.mx/web2/pop/seriacion0253.html
http://www.fca.unam.mx/contaduria_plan_2005.php
http://www.politicas.unam.mx/carreras/ap/curri_ap_05c.pdf
http://www.economia.unam.mx/etsprof/planes/estrucurri.pdf
http://www.quimica.unam.mx/materias.php?id_rubrique=326&id_article=716&color=227AB9&rub2=326
http://www.trabajosocial.unam.mx/licenciatura.htm

http://www.filos.unam.mx/LICENCIATURA/hispanicas/asignaturasYtemarios/mapa_curricular.pdf
http://www.webveterinaria.com/escuelas/planunam.shtml
http://132.248.225.10/licenciatura/plan_de_estudios.htm

Capítulo 6

Auditoría Informática

http://www.docstoc.com/docs/21362280/METODOLOGIAS-DE-CONTROL-INTERNO-SEGURIDAD-Y-INFORMATICA
http://books.google.com/books?id=DwTlt1F_Ac0C&pg=PA46&dq=tipos+de+auditorias+informaticas&hl=es&ei=iLdmTbPiE470tgPHodGmBA&sa=X&oi=book_result&ct=result&resnum=4&ved=0CD4Q6AEwAw#v=onepage&q&f=false
http://www.34t.com/box-docs.asp?doc=497
http://books.google.com/books?id=OqlSVYn0fI0C&pg=PA265&dq=tipos+de+auditorias+informaticas&hl=es&ei=iLdmTbPiE470tgPHodGmBA&sa=X&oi=book_result&ct=result&resnum=3&ved=0CDkQ6AEwAg#v=onepage&q&f=false
http://vbarreto.ve.tripod.com/keys/audi/audi02.pdf

Bases de Datos espejo

http://books.google.com.mx/books?id=wDL0VJNT4EkC&pg=PA93&dq=sistema+espejo+en+bases+de+datos&hl=es&ei=oAyUTdzMYycsQOKxqHGBQ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCgQ6AEwAA#v=onepage&q=sistema%20espejo%20en%20bases%20de%20datos&f=false

Código deontológico

http://tecic.com.ar/Etica_codigos.html

CRAMM

http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

Delitos informáticos

http://www.revistaciencias.com/publicaciones/EkpAEykklAXFAejETp.php

Disponibilidad de la BD

http://www.osmosislatina.com/aplicaciones/bases_de_datos.htm

EBIOS

http://www.isdecisions.com/es/conformidad/metodologica/octave.cfm
http://dspace.ups.edu.ec/bitstream/123456789/573/4/CAPITULO2.pdf

Enfoques de la Auditoría informática

http://jrvargas.files.wordpress.com/2009/03/conceptos-basicos-de-auditoria-informatica.pdf

Ética informática

http://tecic.com.ar/Etica_contenidos.html
http://www.tipete.com/userpost/topics/la-etica-de-la-informatica

Fases de una Auditoria

http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm

Filtrado de direcciones MAC

http://es.scribd.com/doc/23647929/Redes-Inalambricas

Herramientas que verifican la integridad del sistema

http://www.netzweb.net/html/print/segurid/her_mon.pdf
http://insecure.org/tools/tools-es.html
http://webcache.googleusercontent.com/search?q=cache:srOtlU6luVMJ:lasfiguritas.com/moodle/+herramienta+IFSTATUS&cd=13&hl=es&ct=clnk&lr=lang_es&source=www.google.com
http://www.rediris.es/cert/tools/index.html.es
http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

Bibliografía

ISO 27000

www.iso.org
http://www.iso27000.es/iso27000.html#section3b
http://www.iso27000.es/iso27000.html#section3c

Kerberos

http://web.mit.edu/kerberos/

Legislación Internacional.

http://www.segu-info.com.ar/delitos/alemania.htm
http://www.segu-info.com.ar/delitos/austria.htm
http://www.segu-info.com.ar/delitos/chile.htm
http://www.segu-info.com.ar/delitos/china.htm
http://www.segu-info.com.ar/delitos/espania.htm
http://www.segu-info.com.ar/delitos/estadosunidos.htm
http://www.segu-info.com.ar/delitos/francia.htm
http://www.segu-info.com.ar/delitos/holanda.htm
http://www.segu-info.com.ar/delitos/inglaterra.htm

MAGERIT

http://alarcos.inf-cr.uclm.es/doc/psi/Resumenes-Trabajos.pdf
http://www.coit.es/publicac/publbit/bit128/bitcd1/legisla/pg5m21.htm

Mecanismos de seguridad

http://pilaxo.galeon.com/TEMA_9-bd.pdf

Objetivos MAGERIT

http://www.csi.map.es/csi/pdf/magerit_v2/metodo_v11_final.pdf

OCTAVE

http://dspace.ups.edu.ec/bitstream/123456789/573/4/CAPITULO2.pdf
http://www.isdecisions.com/es/conformidad/metodologica/octave.cfm
http://www.utpl.edu.ec/eccblog/wp-content/uploads/2007/04/articulo-tecnico-evaluacion-de-amenazas-y-vulnerabilidades-de-recursos-criticos-operacionalesoctave-a-nivel-de-usuario-final-para-la-utpl.pdf
http://secugest.blogspot.com/2008/11/metodologias-de-analisis-de-riesgos.html

Otras legislaciones

http://www.segu-info.com.ar/legislacion/

Principales amenazas de seguridad

www.wilac.net/tricalcar

Seguridad en Bases de Datos

http://pilaxo.galeon.com/TEMA_9-bd.pdf
http://www.maestrosdelweb.com/principiantes/%C2%BFque-son-las-bases-de-datos/
http://www.itescam.edu.mx/principal/sylabus/fpdb/recursos/r1335.PDF