UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

T E S I S

PORTAL DE SEGURIDAD INFORMÁTICA

QUE PARA OBTENER EL TÍTULO DE :
INGENIERA EN COMPUTACIÓN

P R E S E N T A:
ERIKA LÓPEZ LÓPEZ

DIRECTORA DE TESIS:
M.C MARÍA JAQUELINA LÓPEZ BARRIENTOS

CIUDAD UNIVERSITARIA, MÉXICO D.F. 2013

DEDICATORIAS

Dedico la presente tesis a:

Mis padres:

Antonio J López y Graciana E López *por todo su amor, por sus consejos, sus valores, porque creyeron en mí y porque me sacaron adelante, dándome ejemplos dignos de superación y entrega, porque en gran parte gracias a ustedes, hoy puedo ver alcanzada mi meta, ya que siempre estuvieron impulsándome en los momentos más difíciles de mi carrera, y por ese orgullo que sienten por mí, el cual fue lo que me hizo llegar hasta el final, gracias por darme una carrera para mi futuro, todo esto se los debo a ustedes.*

*Mis hermanos**:***

Catalina *por ser el mejor ejemplo de una hermana mayor,* ***Juan Carlos y José Antonio,*** *por estar conmigo y por apoyarme en cada momento de mi vida, los quiero mucho.*

*Mis hijos**:***

Yuritza y Daniel *por su amor, comprensión y paciencia, pero sobre todo por ser la alegría de mi vida y fuente de inspiración para seguir adelante y nunca rendirme y así poder ser un ejemplo para ustedes, los amo mucho.*

Héctor:

Que al haberme puesto ante una elección muy difícil, me permitió darme cuenta que lo más valioso eran mis estudios, los cuales serán mis mejores armas para enfrentarme a la vida. Y por acompañarme finalmente a la conclusión de los mismos.

A mis amigos:

Rosalba, Gaby, Guillermo, Juan Carlos, Jorge Padilla, Jorge García, Hugo, *por apoyarme y ser parte de cada una de las diferentes etapas de mis estudios, y a todos aquellos que de un modo u otro me ayudaron en muchos aspectos, sin ustedes difícilmente habría alcanzado este logro.*

AGRADECIMIENTOS

*Agradezco a la **Facultad de Ingeniería de la UNAM,** por permitirme cursar mis estudios de licenciatura, por proporcionándome todo los conocimientos y las herramientas necesarias para poderme desarrollar como una ingeniera en el ámbito laboral.*

*Quedo especialmente agradecida con mi directora de tesis la **M.C María Jaquelina López Barrientos** por su gran paciencia, su comprensión ante las diferentes situaciones que se presentaron durante el desarrollo de la tesis, por su ayuda y apoyo que me otorgo en todo momento. Agradezco todos sus comentarios, direcciones, sugerencias y las diferentes correcciones con las que he podido concluir con este trabajo de tesis.*

*Agradezco la valiosa colaboración de los profesores de la Facultad de Ingeniería: **M. C. Alejandro Velázquez Mena,** la **M.C Cintia Quezada Reyes,** el **M. I. Alejandro Padrón Godínez** y del **Ing. Luis Miguel Murguía**, para la creación de diferentes videos de temas de Seguridad Informática, gracias por el tiempo que dedicaron para su elaboración y que hoy pueden visualizarse a través del portal de Seguridad Informática.*

*Agradezco a mis sinodales: **Ing. Alberto Templos Carbajal, M. C. Alejandro Velázquez Mena, M. I. Alejandro Padrón Godínez, y la Ing. Lucila Patricia Arellano Mendoza,** por su tiempo para la revisión de esta tesis, por sus comentarios y correcciones, misma que me permitieron mejorar y concluir este trabajo de tesis.*

*Agradezco al **laboratorio de Redes y Seguridad**, por las facilidades otorgadas para la realización de este trabajo.*

Finalmente quiero agradecer a todas aquellas personas que de una u otra manera me ayudaron durante mi estancia en la licenciatura y durante la elaboración de esta tesis. A todos gracias.

INDICE

INTRODUCCIÓN

El surgimiento de nuevas tecnologías de comunicación e información transforman rápidamente a la sociedad, una de ellas es el surgimiento de Internet, ya que éste se puede considerar que es uno de los cambios más importantes que la sociedad ha experimentado, hoy en día los participantes se encuentran cada vez más interconectados, y esta interconexión se extiende a más allá de las fronteras nacionales. Al mismo tiempo Internet forma parte de la infraestructura operativa de los sectores estratégicos como: gobierno, salud, educación, comercio y/o industria; desempeña un papel fundamental en la forma en que las compañías realizan sus transacciones comerciales; los gobiernos proporcionan sus servicios a los ciudadanos y a las empresas; las escuelas proporcionan información y servicios a sus estudiantes, personal docente y administrativo, y los ciudadanos se comunican e intercambian información de manera individual.

La naturaleza y el tipo de tecnologías que constituyen la infraestructura de la información y comunicaciones también han cambiado de manera significativa. El número y el tipo de dispositivos que integran la infraestructura de acceso se ha multiplicado, incluyendo elementos de tecnología fija, inalámbrica y móvil, así como una proporción creciente de accesos que están conectados de manera permanente.

Como consecuencia de todos estos cambios, la naturaleza, volumen y sensibilidad de la información que se intercambia a través de esta infraestructura se ha incrementado de manera significativa, en este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes y dispositivos que almacenan la información, por la existencia de personas ajenas a ella, que buscan tener acceso a la red o al dispositivo donde se encuentra guardada la información, para modificar, sustraer o borrar datos.

La información se convierte en un activo muy valioso para las personas, las empresas y los países; ya que contiene desde datos personales hasta información financiera que puede ser transformada en capital contable, debido a que existen amenazas que atentan contra la integridad, confidencialidad y disponibilidad de la información. Además las Tecnologías de la Información (TI) contienen vulnerabilidades que pueden ser aprovechadas por atacantes, sin mencionar la cantidad de virus, troyanos, sniffers, key loggers que se encuentran en la red.

Por lo que surge la necesidad de desarrollar una “cultura de seguridad” en donde se cree una mayor conciencia y entendimiento en el uso de la interconexión de sistemas y redes de información. Los sistemas, redes y servicios de información afines, deben ser fiables y seguros, dado que los participantes son cada vez más dependientes de éstos. Sólo un enfoque que tome en cuenta los intereses de todos los participantes y la naturaleza de los sistemas, redes y servicios puede proporcionar una seguridad efectiva.

Entendiendo por Seguridad aquellas reglas, técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible a robo, pérdida o daño, ya sea de manera personal, grupal o empresarial, garantizando que los recursos informáticos estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos.

Es necesario crear espacios virtuales que proporcionen información necesaria y que amplíen los conocimientos sobre seguridad informática para que de esta forma las personas que hagan uso de la Web cuenten con los conocimientos y herramientas mínimas para enfrentar las amenazas y vulnerabilidades que puedan afectar la información. Y donde se publiquen las investigaciones que se realizan en las instituciones educativas.

Ya que los países desarrollados han tomado la delantera en la publicación de espacios dedicados a la seguridad; y al buscar dentro de la red**,** nos encontramos con que la mayoría de los contenidos se encuentra en inglés, la escasa información en español proviene de España, pareciera que países latinoamericanos no generan investigación en este campo pero la realidad es otra, no es la falta de investigación sino la ausencia de divulgación. Esto quedó reflejado en el congreso de Internet 2007 celebrado en El Instituto de Investigaciones Filológicas de la UNAM (IIFL) dentro de los grandes puntos que se abordaron se discutió la poca participación de la sociedad mexicana en la creación de contenidos informáticos. Pero se llegó a concluir que el problema no radica en la generación de contenidos, sino que está realmente en la publicación de estos, ya que no disponemos de una cultura adecuada para mostrarlos al mundo.

Por ello surge la elaboración de la presente tesis, la cual tiene como objetivo principal el desarrollar un portal de seguridad informática para la Facultad de Ingeniería de la UNAM, donde se proporcionen los conocimientos necesarios para protegerse de personas o procesos no autorizados que atenten contra la seguridad de la información. Para lograrlo debemos sensibilizar a los usuarios acerca de la importancia de la seguridad, mostrando el panorama actual de los procesos de IT (Tecnologías Informáticas) en nuestro país; enfrentando las diferentes amenazas y vulnerabilidades que se presentan en los sistemas y procesos de tecnologías de información que existen actualmente, y contrarrestar las que surjan día a día. Por lo que debemos revisar los estándares internacionales de seguridad informática que nos permitan orientar la selección de herramientas adecuadas que cumplan con el fin de proteger la información. Con ello tratamos de crear grupos de personas informadas, así como de personas que se preocupen por la seguridad informática y que de esta forma exista una cultura de la seguridad.

Y que a través de los diferentes elementos contenidos en el portal de Seguridad Informática permita:

- Sensibilizar al público en cuanto a la importancia de la necesidad de proteger la información personal y de las instituciones.

- Revisar y analizar la situación actual de la Seguridad Informática en México
- Informar que la seguridad informática es un camino no un fin.
- Conocer las medidas mínimas para comenzar a enfrentar las amenazas y vulnerabilidades,
- Mostrar un panorama general de las amenazas y vulnerabilidades que se presentan en los ambientes de red y los mecanismos para poder enfrentarlos.
- Conocer la importancia, los conceptos y fundamentos teóricos de la Seguridad Informática
- Revisar y analizar los estándares nacionales e internacionales sobre Seguridad Informática.
- Proporcionar documentos que sean de utilidad para reafirmar o ampliar la información.
- Mantener informados a los usuarios para que puedan tomar sus precauciones necesarias.
- Mostrar las diferentes metodologías para desarrollar esquemas de seguridad y administración de la seguridad.
- Proporcionar herramientas de seguridad y ligas a sitios de interés.

Para ello es que en el capítulo 1 del presente trabajo se presenta el marco teórico, donde se da una breve historia de internet y de la evolución de la Web, la cual nos permitirá revisar los diferentes elementos que han surgido con la nueva Web y de esta forma identificar aquellos elementos que puedan integrarse al portal web, en el capítulo 2 se muestra el análisis correspondiente para llevar a cabo el portal de Seguridad Informática, así como el diseño que tendrá el portal tanto en la organización de la información como el diseño visual que tendrá el sitio, en el capítulo 3 se definen los fundamentos de Seguridad Informática como es su evolución histórica, así como la presentación de los diferentes estándares, vulnerabilidades, amenazas y ataque existentes, en el capítulo 4 se muestran los diferentes esquemas de seguridad como son las políticas de seguridad,

los procedimientos y planes de contingencia, los perfiles de protección y el análisis de riesgos, en el capítulo 5 se presentara los aspectos legales que deben legislarse dentro de las leyes Mexicas así como los diferentes códigos de ética que ayuden al comportamiento moral del hombre ante la sociedad y en el capítulo 6 se presenta una lista de las diferentes herramientas de Seguridad Informática indicando sus características principales y el tipo de servicio que protege.

CAPÍTULO 1

Marco Teórico

Dentro de este capítulo se presenta una breve historia del internet, así como de la evolución de la Web a través del tiempo, donde se revisarán los diferentes elementos que la han caracterizado y a partir de ello identificar aquellos que sean pertinentes para su utilización en el portal web de Seguridad Informática.

CAPÍTULO 1

Marco Teórico

1.1 Internet

La red Internet es el resultado de comunicar miles de redes de computadoras entre sí. Permite conectar diferentes tipos de redes, que pueden ser de área local o de área extensa, utilizando protocolos como TCP-IP, que identifican los datos aunque procedan de diferentes tipos de equipos (PC's, Macintosh, Linux, Mac) y usen sistemas operativos anteriormente incompatibles como UNIX, WINDOWS, OS/2, LINUX, etc., (Ferreyra Cortés, 1996), pero lo más importante es que en Internet se comparten e intercambian información millones de personas mediante millones de computadoras conectadas a través de miles de redes en todo el mundo.

Con el programa adecuado se pueden transferir diversos archivos, conectarse de forma remota a una computadora que se encuentra a miles de kilómetros de distancia y utilizar los diversos servicios que nos ofrece hoy en día Internet, como son el correo electrónico, chats, foros, páginas web, entre otros.

Internet afecta todos los aspectos de la sociedad, entre ellos el comercial, educación y de comunicaciones interpersonales, entre otros. Vivimos en un mundo en que la velocidad y la convivencia se han vuelto cosas normales, Bancos, compras y viajes son posibles las 24 horas al día. La comunicación y la información toman un lugar natural en un mundo que enfatiza la gratificación instantánea y el acceso limitado (Eager, 1995).

La comunidad académica ha contribuido de manera significativa a crear los recursos disponibles en Internet. Estudiantes y maestros usan Internet para ayudarse en tareas que van desde escribir informes hasta preparar cursos.

1.2 Historia del internet

Internet fue concebido en 1969, cuando la Agencia de Proyectos de Investigación Avanzada (ARPA, una organización del Departamento de Defensa de Estados Unidos) patrocinaba investigación en redes computacionales. La investigación se centraba en la creación de redes de intercambio de paquetes, un sistema en que la información (mensaje o archivos) se descomponen en pequeños paquetes que se mueven de manera independiente entre varias redes hasta alcanzar su destino, y cuando todos han llegado se ensamblan (Eager, 1995).

Esta investigación en redes computacionales contemplaba diversos objetivos. El militar era crear un sistema estadounidense de comunicaciones que fuera impenetrable ante los ataques de otros países (en especial la ex Unión Soviética). El nuevo sistema, conocido como ARPANET, prometía mantener integridad de la comunicación en el caso de emergencia en Estados Unidos. En ARPANET la información se movía de manera aleatoria por diferentes redes y sistemas en lugar de viajar sobre una línea y llevar a un punto central de intercambio o concentrador.

De manera fundamental, la idea era: construir una red para investigadores a todo lo largo de Estados Unidos, para que pudieran utilizarla en sus actividades diarias y, además tuvieran la seguridad que la destrucción de una máquina en una localidad no detendría la funcionalidad de la red. Como localizador de pruebas se establecieron cuatro servidores ARPANET: la Universidad de Utah, el Instituto de Investigaciones de Stanford (Stanford Research Institute) y dos servidores de la Universidad de California, Santa Bárbara y los Ángeles. En septiembre de 1969, se conectó ARPANET (Randall, 1994).

En otoño de 1972, más de un millón de personas presenció la primera demostración pública de ARPANET y entonces fue cuando verdaderamente la idea de una red nacional (e incluso internacional) empezó a cobrar forma. Todos empezaron a encontrar razones por las que tenían que formar parte de la misma (Randall, 1994).

Los creadores de este sistema tuvieron el cuidado de desarrollar reglas voluntarias que cubrieran todos los aspectos d este sistema. Se hicieron estándares para la creación de direcciones y para los protocolos de comunicaciones (Ferreyra Cortés, 1996).

Por lo que se hicieron dos decisiones técnicas que hicieron posible el funcionamiento de la red, éstas fueron desarrollo de la tecnología de la conmutación por paquetes y el diseño de TCP/IP.

La conmutación por paquetes hace posible que los datos provenientes de diferentes máquinas compartan líneas de transmisión comunes. Sin esto, serían necesarias, o por lo menos preferibles, las líneas dedicadas que enlazaran una computadora directamente con otra (esto es, una máquina o una red con otra máquina o red) con los datos direccionados a través de los nodos, en función de su origen y destino.

La tecnología de conmutación por paquetes divide los datos en pequeños *paquetes,* cada uno de ellos con un código que contiene el destino y las instrucciones para reconstruir la información. Los paquetes se mueven en forma individual a través de la red y se reúnen de nuevo cuando todos llegan a su destino.

TCP/IP son las siglas de Transmission Control Protocol/Internet Protocol (Protocolo de Control de Transmisión/ Protocolo Internet), esta tecnología fue desarrollada a mediados de los años setenta, y proporciona el medio estándar mediante el cual las computadoras pueden comunicarse unas con otras, ya que el protocolo de la computadora establece procedimientos que permiten una comunicación efectiva (Randall, 1994). TCP/IP fue parte de una investigación del DARPA sobre la conectividad de diferentes tipos de computadoras y redes. Debido a que usaron fondos públicos para desarrollar TCP/IP, los estándares son no propietarios; esto es, que nadie tiene derechos exclusivos de uso.

Además, TCP/IP es hardware y software independientes, de manera que cualquier tipo de computadora puede conectarse a Internet y compartir información con otras computadoras (Eager, 1995).

En 1975, la Agencia de Comunicaciones de la Defensa de Estaos Unidos obtuvo control administrativo de ARPANET. La misión de la agencia era satisfacer las necesidades de comunicación del Departamento de la Defensa. El tráfico de la red se incrementaba con gran rapidez. La mayoría de los usuarios no eran personal militar sino investigadores que usaban en gran medida la red para enviar correo electrónico y transferir archivos a sus colegas. Debido a esta aplicación dual, ARPANET se dividió en dos redes: ARPANET continuó sirviendo a las necesidades de la comunidad académica, mientras MILNET se enfocó a los requerimientos militares. La información podía ser compartida entre estas dos redes. La interconexión entre ARPANET, centrada en la investigación, y MILNET, orientada a las aplicaciones, empezó a conocerse como DARPA Internet (Agencia de Proyectos de Investigación Avanzada de la Defensa), casi siempre llamada Internet.

En 1986, la Fundación Nacional de Ciencias (NSF) contribuyó de manera significativa a la expansión de Internet, al desarrollar una red que conectaba a investigadores de Estados Unidos con diversos centros de supercomputadora. De acuerdo a (Eager, 1995) en estos centros se incluían los siguientes:

- Supercomputadora Nacional de Cornell, Universidad de Cornell, Cornell, Nueva York.
- Centro Nacional de Supercómputo de John Von Neumann, Princeton, Nueva Jersey
- Centro Nacional para Aplicaciones de Supercómputo (NCSA), Universidad de Illinois, Champaign, Illinois.
- Centro de Supercómputo de Pittsburgh, Pittsburgh, Pensilvania.
- Centro de Supercómputo de San Diego, Universidad de California, San Diego, California.
- División de Cómputo Científico del Centro Nacional de Investigaciones Atmosféricas, Boulder, Colorado.

Las redes de alta velocidad que conectaban supercomputadoras de la NSF formaron la columna vertebral de comunicaciones conocida como NSFNET, en la cual las líneas de transmisión incluían teléfono, fibras ópticas y enlace por satélite. Estas líneas de transmisión son supercarreteras de datos que llevan tráfico a distancias largas y a velocidades grandes. Fue configurada en un principio con líneas de transmisión de 56Kbps[1] y que se mejoró en 1989 con líneas T-1[2] capaces de transmitir a velocidades de 1.5 Mbps (megabits por segundo), este tipo de conexión aún sigue en funcionamiento

[1] **Kbps** (Kilobits por segundo), unidad de medida que se usa en telecomunicaciones e informática para calcular la velocidad de transferencia de información a través de una red.

[2] **T-1** es el servicio de línea digital normalizado, el cual se originó de una necesidad de más ancho de banda.

pero, en 1990, se introdujo la especificación T-3, lo que permitió velocidades de conexión de hasta 45 Mbps.

A finales de los ochentas, NSF pasó el financiamiento y la administración de la NSFNET a un grupo no lucrativo de universidades, llamado MERIT (Michigan Educational Research Information Triad). MERIT trabajó junto con MCI e IBM en la expansión y la mejora del acceso nacional a alta velocidad. Temporalmente, las tres organizaciones formaron la ANS (Advanced Network Services), creada con la finalidad de operar a la NSFNET.

Para 1990, la NSFNET había tomado el lugar de ARPANET y este último había quedado discontinuado. En 1991, el entonces presidente de Estados Unidos, George Bush, firmó la High Performance Computing Act, misma que esencialmente establecía una nueva red, la NREN (National Research and Education Network). La NREN iba a utilizar a la NSFNET como su base e irónicamente con metas de investigación similares a las de ARPANET original. La NREN fu establecida en forma específica para reunir organizaciones gubernamentales y comerciales, lo que vino a significar que la política no comercial de NSFNET ha desaparecido en su mayor parte (Randall, 1994).

Mientras ocurría todo esto, otras organizaciones comenzaban a interesarse en las redes globales y es como la CSNET (Computer Science Network) fue establecida por la NSF para ayudar a las universidades que no podían tener acceso a la NSFNET e introducirlas en lo que poco a poco se convertiría en Internet. Sin embargo, la única herramienta que esta nueva red podía utilizar, era el correo electrónico, lo cual tenía sus limitaciones. Apareció otra nueva red, la cual se llamó BITNET la cual ofrecía servicio de correo electrónico, listas de correo, capacidades de transferencia de archivos y otras opciones. Desafortunadamente, BITNET no utilizaba el TCP/IP, por lo que tuvo que desarrollar otra forma para compartir la información con NSFNET. Finalmente, BITNET y CSNET se dieron cuenta que estaban intentando llevar a cabo prácticamente lo mismo (esto es, conectarse a NSFNET) por lo que formaron la CREN (Corporation for Research and Education Networking).

Con la finalidad de no quedarse a tras otras partes del mundo decidieron conectarse a la red emergente. Canadá estableció el CAT*NET y el NETNORTH, el primero corresponde aproximadamente a NSFNET y el segundo a BITNET. Las redes europeas empezaron a organizarse también, de las cuales EARN Y EUNet son los ejemplos principales. Con Sudamérica, el Oriente Medio, Australia y la Franja del Pacífico Sur con un interés activo en Internet, (Randall, 1994), fue solo cuestión de tiempo para que las redes nacionales o continentales se unieran para que así surgiera el término *Internet* el cual se refería originalmente a los experimentos de ARPA en redes internacionales, y que hoy en día conocemos como la red de redes.

Desde 1993 Internet deja de ser la red de instituciones gubernamentales y universidades para convertirse en la red pública más grande del mundo. A partir de entonces han aparecido y aumentado los servicios de conexión como Prodigy, CompuServe y Amerian Online en Estados Unidos; Spin, CompuServe, Internet de México, PixelNet Y Datanet en México y algunos más en otros países (Ferreyra Cortés, 1996).

1.3 WWW

El servicio gráfico de la gran red se conoce como **World Wide Web**, también conocida como **WWW, W3,** *telaraña mundial,* en general se denomina **Web** para simplificar las menciones a este sistema de localización de computadoras anfitrionas o *lugares con servidores* World Wide Web (Web sities), en donde se ofrece información, archivos y ligas de hipertexto hacia otros archivos y ligas de hipertexto hacia otros del mismo nodo o hacia otros lugares. (Ferreyra Cortés, 1996)

La tecnología de la comunicación facilita la conectividad global, y el WWW es un medio funcional para que la gente de todo el mundo localice información y comparta el conocimiento. El WWW es según (Eager, 1995):

- Un sistema de navegación para Internet
- Un sistema de administración y distribución de información
- Un formato dinámico para la comunicación masiva personal

La Web integra diferentes formatos de información: imágenes fijas, imágenes en movimiento, texto, audio y video.

1.4 Historia del web

El Word Wide Web es un sistema distribuidor de información basado en el concepto de hipertexto. Fue desarrollado por un grupo de investigadores bajo la dirección de Tim Berners-Lee, en el Laboratorio Europeo de Física en Partículas, CERN, ubicado en Suiza (Ferreyra Cortés, 1996). La comunicación eficaz era decisiva para este grupo de científicos localizados en todo el mundo. La propuesta definía un sistema simple que usara hipertexto, una forma de presentar y relacionar información con enlaces en lugar de líneas secuenciales, para transmitir documentos y comunicación por las redes de cómputo. Al principio, el programa no preveía transmitir imágenes o incluir audio y video.

A fines de 1990, se introdujo el primer software Web en una computadora NeXT de Steve Job's. El software NeXT permitía ver y transmitir documentos de hipertexto en Internet y facilitaba la edición a los usuarios. Se hicieron demostraciones de este sistema en los comités del CERN y ante los asistentes a la "Conferencia de hipertexto" del 1991. En los años siguientes, el sistema Web se expandió con rapidez (Eager, 1995).

El crecimiento anual de Web fue tan sorprendente que en 1993, existían alrededor de cien servidores Web; hoy en día la Web tiene más de 612, 843,420 servidores (figura 1.1). Así también podemos observar cómo fue evolucionando la WWW en la siguiente línea del tiempo de acuerdo a Eager (1995), donde muestra los sucesos más importantes (figura 1.2).

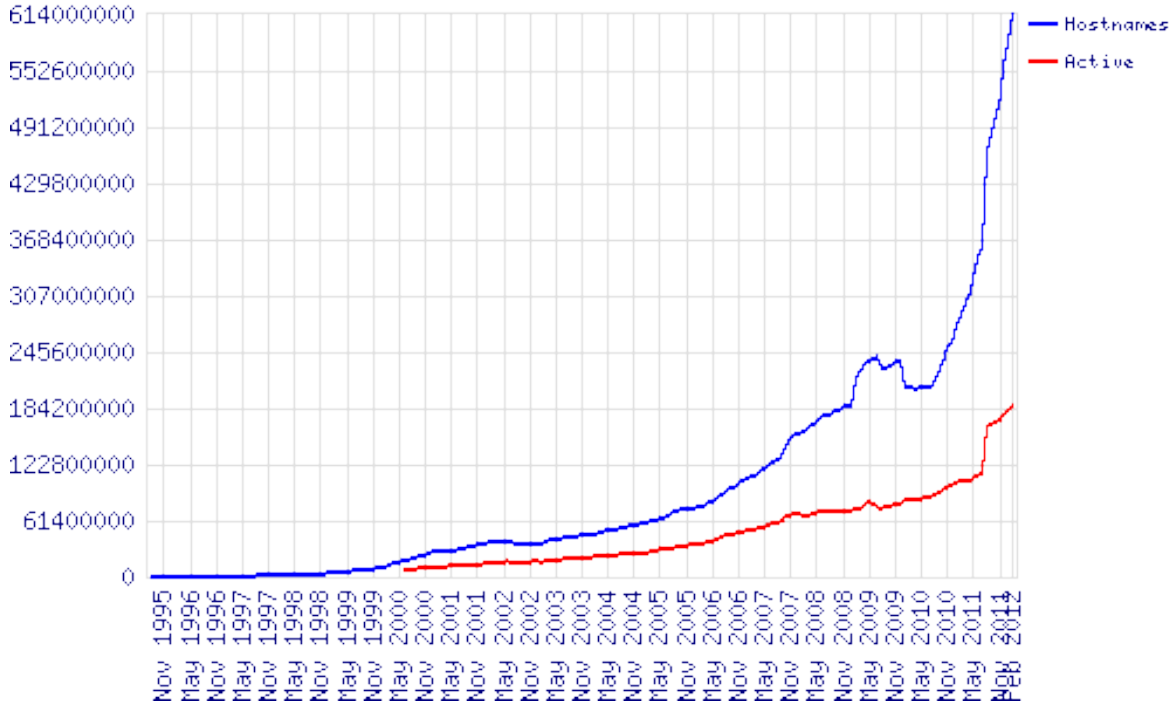


Figura 1.1. Total de Sitios en todos los dominios de Agosto de 1995 hasta Febrero del 2012 (Netcraft, 2012).

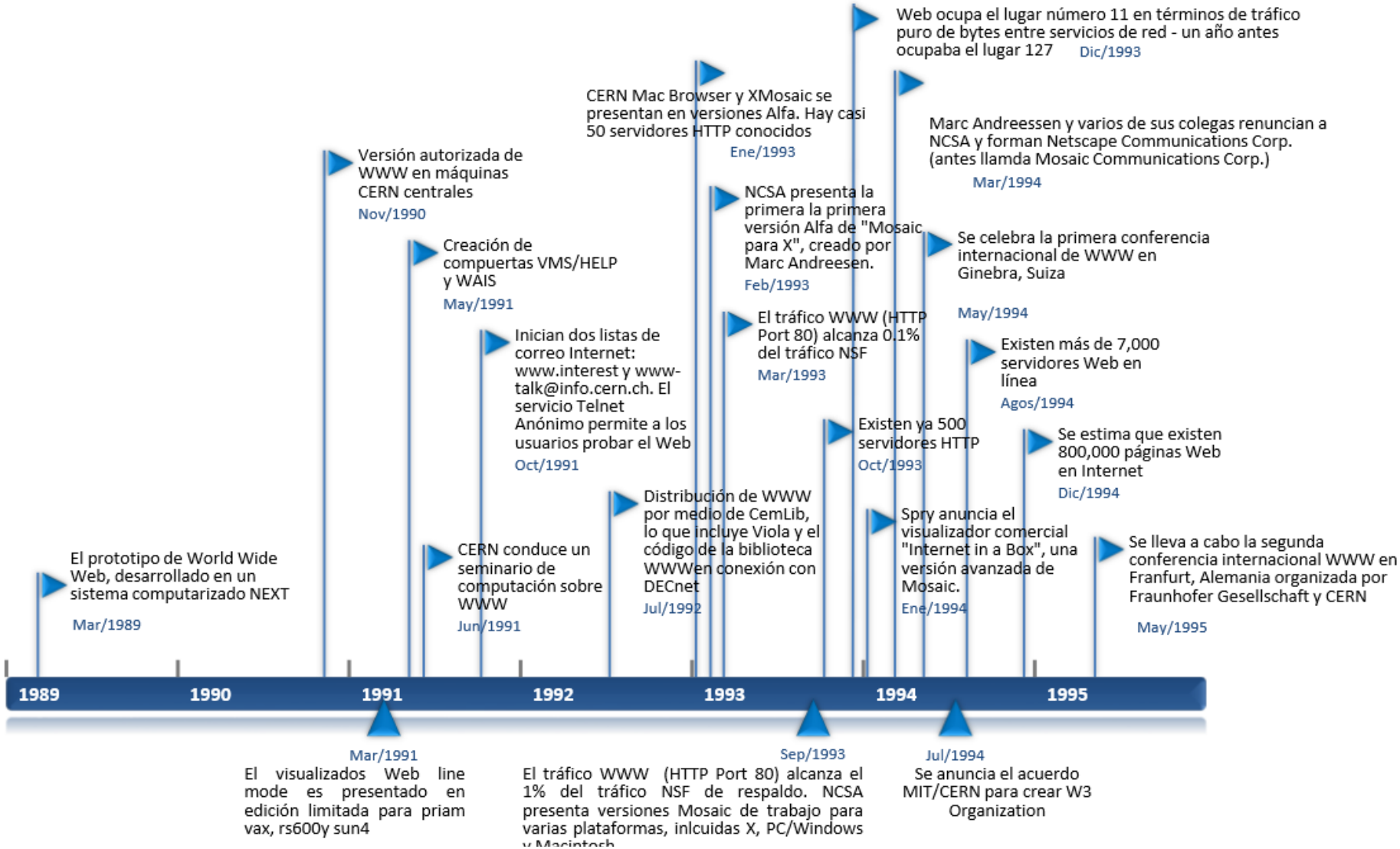


Figura 1.2 Línea del Tiempo del WWW. Sucesos importantes en la corta vida del Web (Eager, 1995) pg.43

El WWW alcanza su máxima popularidad en 1993 con la aparición del primer software de fácil uso para navegar en el Web, Mosaic. Este tipo de programas se conocen como visualizadores (Browsers) u hojeadores del Web, ya que las interfaces de los clientes y servidores de estos servicios se les conocen como páginas web (Eager, 1995).

1.4.1 Los conceptos de hipertexto e hipermedia

Los programas de información computacional que posibilitan la navegación en la WWW son el hipertexto e hipermedia.

El *hipertexto*, un subconjunto de hipermedia, se refiere de manera específica a documentos computacionales donde los lectores se pueden mover de un lugar a otro, de un documento a otro o entre documentos, de una manera no secuencial ni lineal, ya que se puede desplazar en forma aleatoria. Las palabras, frases e iconos del documento se convierten en enlaces que permiten viajar a una nueva posición en el mismo documento o, incluso, a uno nuevo (Eager, 1995).

De acuerdo a Eager, el hipertexto tiene varias ventajas sobre el texto el texto normal:

- El hipertexto facilita navegar en documentos muy largos.
- Además de la velocidad de uso, el hipertexto ayuda a los lectores a explorar nuevas ideas y localizar nuevas fuentes de información, a medida que se desplaza de lugar a lugar.
- Brinda profundidad, como una especie de tercera dimensión, a la palabra escrita. Los lectores se convierten en exploradores y toman decisiones de navegación acerca de los temas que desean investigar. El hipertexto permite al usuario decidir de manera precisa qué información es la más importante en un momento dado.

Hipermedia es una extensión natural de hipertexto. En hipermedia, los enlaces son conexiones visuales a gráficas o fotografías, mensajes de audio o video, así como a texto. Hipermedia le da vida a un documento y la computadora personal de convierte es un dispositivo multimedios que pueden ser más atractivo e impresionante que la radio o televisión. (Eager, 1995)

El HTML (HyperText Markup Languaje) consiste propiamente en un archivo de texto con códigos que especifican en cada parte de él, si se trata de texto, gráficos, videos o sonido. Además se resaltan palabras o partes del texto y que desde ahí se puedan realizar "saltos" hacia otra parte del mismo archivo, hacia otra página; algunos de estos enlaces de hipertexto pueden activar un sonido o voz, en un proceso conocido como hipermedia.

El principio del HyperText Markup Languaje fue un gran avance, pero no significaba más que poner al alcance del cliente, los servicios de texto y gráficas sobre una interfaz tipo terminal; es decir en modo texto (Ferreyra Cortés, 1996).

Los vínculos de hipertexto se pueden señalar con un color en el propio texto o en las imágenes. Al posicionar el apuntador del ratón sobre de ellos, cambia la forma de la flecha indicando que se puede accesar a esa liga. Para señalar los vínculos que ya han sido visitados, el texto que hace la liga de color. (Ferreyra Cortés, 1996)

1.5 La nueva web

Los sitios Web ya no son soló texto e hipervínculos. Son imágenes, animaciones Flash, publicidades que tapan la lectura, ventanas desplegables, videos, juegos y aplicaciones completas. Es por eso que la Web como la conocíamos ha cambiado debido a la aparición de una nueva Web, la Web 2.0.

Siempre que se habla de la Web 2.0, se acostumbra a poner como ejemplo ilustrativo a una serie de servicios que se ofrecen a través de la Web, que se caracterizan por ofrecer una interfaz especialmente ágil y flexible, como pueden ser todos los servicios ofrecidos entre otros por las grandes empresas de Internet como Google con GMail, Spreadsheets&Docs por ejemplo o los ofrecidos por Yahoo! tipo Flicker, del.icius, etc. Detrás de esas aplicaciones, cabría identificar como común denominador la tecnología AJAX (Asynchronous Javascript And XML). Bajo este acrónimo, se esconde una combinación creativa de tecnologías, que permite agilizar la interacción entre el navegador y el propio usuario.(Fumero, Roca, & Sáez Vacas, 2007).

1.5.1 ¿Qué es la nueva Web?

La Web dos (punto) cero podría definirse como la promesa de una visión realizada: la Red convertida en un espacio social, con cabida para todos los agentes sociales, capaz de dar soporte a y formar parte de una verdadera sociedad de la información, la comunicación y/o el conocimiento. (Fumero, Roca, & Sáez Vacas, 2007)

Es un concepto abierto que abarca tres grandes nociones de acuerdo a Firtman (2010):

1. Aplicaciones Ricas de Internet
2. Web semántica
3. Redes sociales

1.5.2 Historia de la Nueva Web

El término Web 2.0 tiene un origen claro: fue utilizado por primera vez por O'Reilly Media (empresa conocida por su editorial de libros de tecnología) en una conferencia en Octubre del

2004. Meses después fue Tim O'Reilly fundador de la empresa quien definió el concepto y lo hizo conocido en la comunidad (Firtman, 2010).

Figura 1.3 Diagrama de conceptos que asocian a la Web 2.0. Diagrama distribuido bajo la licencia libre conocida como Creative Commons

De acuerdo a Firtman (2010), en ese momento la definición de O'Reilly incluía:

- La Web como plataforma
- Efectos de red en una arquitectura de participación
- Innovación y desarrolladores independientes
- Pequeños modelos de negocio capaces de publicar servicios y contenidos
- Datos abiertos
- El perpetuo Beta

1.5.3 ¿Que no es la Web 2.0?

- La Web 2.0 no es Internet 2. Este último concepto es una red paralela de alta velocidad utilizada por universidades. Web 2.0 funciona sobre la misma red de Internet que todos conocemos.

- Tampoco es un nuevo lenguaje de programación

- Web 2.0 no es un cambio radical de tecnología, ya que se sigue utilizando HTTP, HTML, JavaScript y muchas con las tecnologías que se habían estado trabajando, solo que se utilizarán de un modo distinto.

- Tampoco es solo AJAX, RSS, ni blogs, ni ningún concepto suelto.

1.5.4 WEB 1.0

La web 1.0 había evolucionado desde 1995 durante 10 años, se le cataloga como la que falló en la conocida burbuja de Internet, a finales del milenio pasado en la que cientos de miles empresas punto com debieron cerrar sus puertas luego de millones de dólares invertidos (Firtman, 2010).

En la siguiente tabla se comparan ambos paradigmas, para facilitar la comprensión del concepto entre las Web 1.0 y la Web 2.0.

Tabla 1.1. Comparación entre los paradigmas de la Web 1.0 y la Web 2.0 (Firtman, 2010)

CONCEPTO	CÓMO ES EN LA WEB 1.0	CÓMO ES EN LA WEB 2.0
Quiénes publica	Los productores de los sitios web	Tanto los productos como los mismo usuarios
Distribución de la información	Centralizada en un sitio Web a través de interconexiones	Dispersa en miles de sitios
Publicidad en la Web	Solo para grandes presupuestos y con campañas cerradas	Cualquiera puede publicar y organizar su propia campaña
Dueños de la información	El sitio web	Los usuarios
Tecnología reinante	HTML 4.0	XHTML, HTML 5 y CSS
Disponibilidad de nuevos servicios Web	Cuando estaban finalizados luego de años de trabajo	Se liberan en modalidad Beta, apenas tengan una funcionalidad
Posibilidad de utilizar servicios de otros sitios	Ninguna	Los sitios ofrecen API abiertas para que otro se conecten

1.5.5 Rich Internet Aplications (Aplicaciones Ricas de Internet)

Una aplicación Rica de Internet es un cruce entre las aplicaciones Web y las de escritorios, que deriva en cierto comportamiento hacia el cliente, que se comunica con el servidor sólo en casos necesarios. El término lo designó en 2002 la empresa Macromedia, en la actualidad Adobe, creadora de la herramienta Flash. En ese momento, Macromedia anunciaba que con su plataforma flash era posible crear una nueva experiencia en los sitios Web que no era posible con HTML y promovió el uso de este nuevo concepto. Tuvieron que pasar varios años antes de que realmente se empezaran a utilizar estos conceptos y su plataforma Flash se volvería una de las principales rivales de AJAX en el mercado.

Figura 1.4Esquema de los participantes en el mundo de las Aplicaciones Ricas de Internet (Firtman, 2010) pág.7

Si se engloban las características de los conocidos como clientes ricos (aplicaciones de escritorio, como Microsoft Excel o Adobe Photoshop) y las de los denominados clientes livianos (aplicaciones Web tradicionales) quedan conjunto con las siguientes características:

- **Experiencia rica del usuario.** Implica hacer uso de nuevos conceptos en la Web, como contrales ricos de ingreso (selectores de fecha, deslizadores, ingreso de texto con formato), servicios de drag y drop y evitar y evitar demoras al usuario en el uso del sitio Web.

- **Capacidad *offline.*** Permite que una aplicación Web siga funcionando aunque se haya perdido la conectividad con el servidor o con Internet. Por supuesto esto será posible en algunos casos; asimismo, si la conexión se retoma seguirá su uso normal.

- **Productividad alta de desarrollador.** Los entornos de trabajo y las herramientas para desarrollar aplicaciones Web evolucionaron hasta encontrarse, en la actualidad, cercas a la productividad en una aplicación de escritorio.

- **Respuesta.** Las aplicaciones Web responden con rapidez y es posible interactuar con la aplicación, aun cuando se espera una respuesta del servidor.

- **Flexibilidad.** Los nuevos sitios Web permiten una interfaz flexible con la posibilidad de modificar la apariencia, el contenido y los servicios disponibles de una manera sencilla y rápida.

- **Fácil de distribuís y actualizar.** Actualizar una RIA es tan simple como publicar los nuevos archivos en el servidor, incluso hasta se podrían actualizar con cientos de usuarios conectados.

- **Fácil de administrar.** No hay metodologías de instalación complejas, DLL ni instaladores.

En una RIA, el cliente adquiere un uso más intensivo, no solo para pequeños validaciones. El *browser* también administrará el flujo de la aplicación, los módulos y la interacción con el servidor. Todas las comunicaciones al servidor no será invocada en forma directa por el clic del usuario, si no por el código de cliente. Estas peticiones al servidor se harán detrás de escena, o sea, el usuario no será consciente de la petición, a no ser que se active de manera explícita un cartel que indica cargando (figura 1.5).

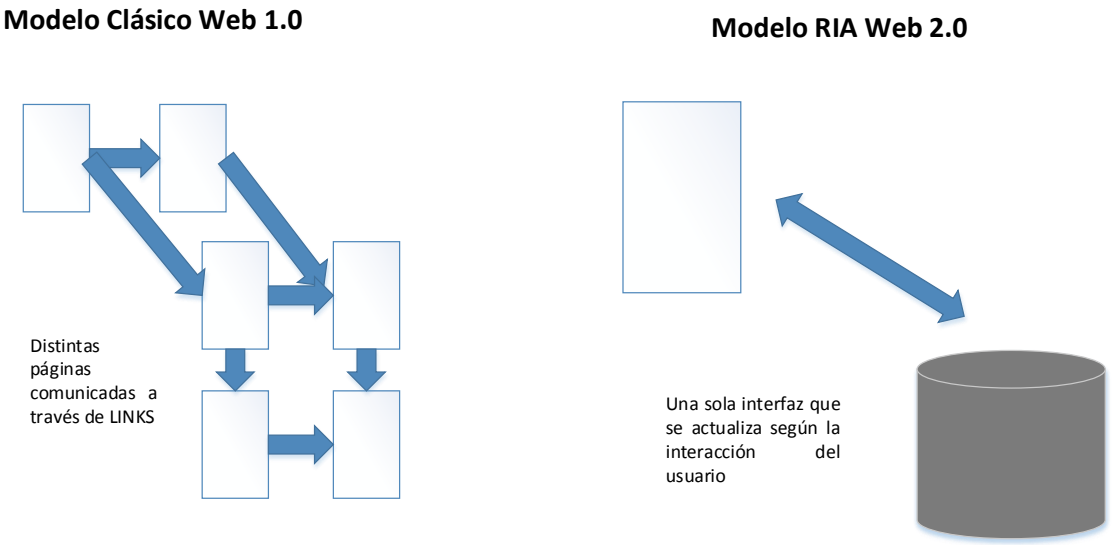


Figura 1.5 Modelo clásico versus modelo de Aplicación Rica de Internet (Firtman, 2010) pág. 10

Ventajas

- Ofrece al usuario una experiencia más rica con el sitio Web

- Están al día con las nuevas expectativas de los usuarios

- Ahorrar tiempo de carga de la página, la cantidad de bytes transferidos y tiempo de navegación total

Desventajas

- **Capacidad de uso.** El usuario hace, por lo menos, 10 años que navega por Internet y eso implica que sabe cómo utilizar un sitio Web 1.0 sin problemas. Sabe que debe ir haciendo clic en hipervínculos, que debe esperar cada recarga, sabe completar un formulario con campos de texto y lista de selección y está acostumbrado al famoso botón Enviar. Ahora bien, ¿Sabrá utilizar el nuevo el sitio Web 2.0 enriquecido?.

  Es necesario educar al usuario acerca de cómo utilizar la aplicación.

- **El botón "Atrás" del navegador.** Todos conocemos el historial de un navegador. Con cada clic en el botón correspondiente se puede retroceder y volver a una página. Sin embargo, ahora ya no existe el concepto de página, sino que cada clic, en realidad puede conllevar cualquier tipo de acción en el sitio o a la aplicación Web, como abrir un menú o borrar una foto y siempre nos encontramos en la misma página o URL (si lo pensamos con el viejo sistema de trabajo).

- **Indexación de buscadores.** En general una Aplicación RICA presenta una sola URL y con un contenido inicial (leído por el buscador). El contenido restante ya no son páginas aparte, sino que son pequeñas zonas que se actualizan directamente en el cliente según la interacción del usuario. Esto implica que el buscador sólo indexará la página inicial.

- **Favoritos o marcadores.** En la Web2.0 no basta copiar y pegar la dirección que vemos en el navegador para añadirlo a favoritos o a marcadores.

- **Manejo de errores.** En la Web 1.0 el usuario percibía directamente los errores del servidor: 404, cuando la página no existe, 500 cuando el servidor tiene problemas internos, etc. Ahora hay que capturar y actuar ante errores que surjan en el servidor que anteriormente no era posible realizar.

- **Complejidad de desarrollo.** El desarrollar Aplicaciones Ricas lleva un trabajo extra respecto de las aplicaciones tradicionales para la Web, ya que son más complejas de depurar, mantener y actualizar.

Es por ello que la educación, que debería constituirse como un pilar en la construcción de la Sociedad del Conocimiento, es uno de los ámbitos que presenta a la vez más oportunidades y al mismo tiempo más barreras institucionales para sacar partido a las infotecnologías.

1.5.6 Web semántica

Se trata de una corriente, promovida por el propio inventor de la Web [Berners-Lee], y presidente del consorcio W3C, cuyo último fin es lograr que las máquinas puedan entender, y por tanto utilizar, lo que la Web contiene. Esta nueva Web estaría poblada por agentes o

representantes software capaces de navegar y realizar operaciones por nosotros para ahorrar trabajo y optimizar los resultados. Para conseguir esta meta, la Web semántica propone describir los recursos de la Web con representaciones procesables (es decir, entendibles) no sólo por personas, sino por programas que puedan asistir, representar, o reemplazar a las personas en tareas rutinarias para un humano. Las tecnologías de la Web semántica buscan desarrollar una Web, más cohesionada, donde sea aún más fácil localizar, compartir e integrar información y servicios, para sacar partido todavía mayor de los recursos disponibles en la Web (Bravo Santos & Redondo Duque, 2005).

El objetivo de la web semántica es que la información en la Web posea metadatos acerca del significado de los datos que se muestran. Esto implica incluir información adicional en los sitios Web, que no será vista por el usuario y que se expresará en algún lenguaje formal que pueda ser estandarizado y comprendido por herramientas automatizadas, como un motor de búsqueda.

Los formatos más utilizados son RDF (Resource Description Framework) y Microformatos, que añaden características adicionales al código de marcas que utilizamos para nuestro sitio web.

RDF (Resource Description Framework)

RDF fue creado en 1998 y recomendado por W3C en 1999, es acrónimo de Resource Description Framework y es un lenguaje para la representación de la información sobre los recursos en la web (autor de una página web, licencia, etc.), particularmente dirigido para la representación de los metadatos. Es decir, define la sintaxis y modelos de datos para la representación semántica de los datos.

Microformatos

La idea de los *microformats* o Microformatos es generar formatos de contenido con HTML válido en la actualidad, utilizando las propiedades del lenguaje, como pueden ser *class, rel o rev* para proveer información adicional sobre el contenido.

1.5.7 Redes sociales

Uno de los fenómenos de la Web 2.0 es la revolución social adquirida por medio de los nuevos servicios en colaboración de la red. La gestión on line de las redes sociales ofrece una serie de funcionalidades, asociadas a servicios básicos de comunicación y presencia, que han logrado convertirla en un fenómeno en sí misma.

Todo el universo web, se sustenta en una diversidad considerable de aplicaciones y servicios agrupados bajo el concepto de software social, como puede ser blogs, wikis, comunidades, entre otros y que en colaboración entre todos los usuarios de la red es parte fundamental de este hecho y es así que como surgen miles de sitios que ofrecen nuevos servicios en colaboración, que comparten fotos, favoritos, RSS, blogs y música.

Blogs y derivados

Los blogs aparecen en la Red, provocando un fenómeno social debido fundamentalmente a su impacto en la dinámica de los medios de información en Internet. La esencia de tal fenómeno es un mecanismo de publicación sustancialmente más sencillo que los que había disponibles antes de su emergencia.

Un blog o Weblog es una base de datos de artículos ordenados de manera cronológica en modo inverso. Equivale a una bitácora o diario personal donde el dueño ingresa texto, adjuntos y links, y otros usuarios pueden dejar comentarios (Firtman, 2010).

Wikis

Una wiki es un sitio web que permite que sus propios usuarios editen, agreguen y eliminen su contenido. Por lo general, estos sitios no requieren un registro por parte del usuario y se basan en la misma comunidad para que no permita abusos al cambiar información. Es el máximo exponente de una autoría en colaboración, donde todos son autores de contenidos (Firtman, 2010).

RSS (Really Simple Syndication)

El RSS es un formato basado en XML que permite encontrar aquella información que mejor se adapta a lo que el usuario desea, pero también ofrecerla de forma rápida y actualizada.

Los archivos RSS son un nuevo método para obtener y ofrecer información gracias a que contienen metadatos sobre las fuentes de información. Este formato es de gran utilidad para sitios Web que actualicen sus contenidos con frecuencia, ya que permite compartir la información y verla en otros sitios de forma inmediata.

CAPÍTULO 2

Análisis y Diseño del portal de Seguridad Informática

Dentro de este capítulo se presenta el análisis realizado para crear el portal de Seguridad Informática, donde se muestra la función principal que tiene el sitio, el por qué debe realizarse, para quién está dirigido y cómo se logrará que se cumplan dichas funciones. Una vez identificados los puntos anteriores se procede a la determinación de los requerimientos del sistema, así como a la revisión y selección de la metodología de desarrollo. Además se define cada uno de los diseños que son necesarios para la creación del portal de Seguridad Informática.

CAPÍTULO 2

Análisis y Diseño del portal de Seguridad Informática

2.1 Determinación del problema

Elaborar un sitio Web de Seguridad Informática para la Facultad de Ingeniería de la UNAM, dentro de su laboratorio de Redes y Seguridad, que permita ofrecer información especializada sobre temas de Seguridad Informática (SI) a la comunidad, con la finalidad de que estudiantes, profesores, investigadores y público en general tomen conciencia de la importancia de la seguridad de la información y tengan oportunidad de actualizar sus conocimientos en estos temas mediante los conceptos teóricos, a través de la revisión de los diferentes estándares, así como de las herramientas de SI que se proporcionen a través sitio.

2.2 Análisis de las necesidades del sistema

El tema de Tesis a desarrollar tiene como objetivo el crear un portal web de Seguridad Informática en la Facultad de Ingeniería de la UNAM, el cual se encontrará alojado en el sitio del laboratorio de Redes y Seguridad, para conocer el alcance del sitio es necesario responder a las siguientes preguntas:

a) ¿Cuál es la función principal que se realizará en el Portal Web?
b) ¿Para qué se debería realizar esa función?
c) ¿Quiénes pueden utilizar esa función?
d) ¿Cómo puedo lograr esa función?

a) ¿Qué función principal se puede realizar en el Portal Web?

La función principal del portal será proporcionar información sobre temas de SI, donde existirá una investigación teórica realizada sobre los temas de Seguridad, así como de los diferentes estándares que existen hasta hoy en día, las distintas herramientas de seguridad que se han desarrollado al momento, además de permitir descargas y manuales sobre éstas respetando los derechos de autor (Copyright[1]), así como ligas de interés a los diferentes temas de SI.

b) ¿Para qué se debería realizar esa función?

El objetivo de desarrollar el portal de SI, es para crear una cultura de seguridad, así como proporcionar información sobre diferentes temas encausados al resguardo de la

[1] **Copyright:** Derecho que la ley reconoce al autor de una obra intelectual o artística para autorizar su reproducción y participar en los beneficios que esta genere.

información, que sea de ayuda para los estudiantes de la Facultad de Ingeniería, ya que actualmente cuenta con un módulo de salida en Redes y Seguridad en la carrera de Ingeniería en Computación, así mismo para todos aquellos que estén interesados en adquirir o acrecentar sus conocimientos en esta área de gran interés en la actualidad, debido a que hoy en día la tecnología avanza rápidamente y con ello se presentan nuevas vulnerabilidades y amenazas que pueden afectar la seguridad de la información.

c) ¿Quiénes pueden utilizar esa función?

El portal está pensado en que sea utilizado por los estudiantes, profesores, investigadores y público en general interesados en temas de Seguridad Informática, ya que de esta manera, los distintos usuarios pueden ampliar sus conocimientos de seguridad y sobre todo podrán revisar su contenido en cualquier momento, debido a que será accesible desde cualquier lugar, ya que el único requisito será contar con una computadora con acceso a Internet.

d) ¿Cómo puedo lograr esa función?

Para lograr este objetivo, debemos dar a conocer la importancia de la Seguridad Informática así como los conceptos básicos que la comprenden, mediante una redacción clara y amena, asimismo estudiar y conocer las diferentes Herramientas que existen, para proporcionarlas de una manera que sean fáciles de utilizar para el usuario y en cuanto a la actualización sobre los diferentes temas de Seguridad Informática, se pretende que sean hechas a través de las noticias que serán incluidas al portal web a través de un RSS[2].

2.3 Determinación de los requerimientos del sistema

- La información que se proporcione en el portal deberá ser clara y veraz.
- El diseño de la página debe de ser atractivo y amigable a la mayoría de los usuarios.
- La herramientas y servicios que se proporcionen en el sitio deberán estar disponibles.
- El sitio deberá ser portable en al menos dos sistemas operativos.
- Los lenguajes de programación a utilizar deberán de proporcionar en la medida de lo posible un entorno de seguridad.
- Las herramientas proporcionadas serán libres.
- Las diferentes páginas que comprenda el sitio deberán ser ligeras para que no tarden más de 10 segundos en ser visualizadas, sin contar los videos y herramientas que contendrá el sitio, ya que la visualización de éstas dependerá del ancho de banda que utilice el usuario.
- El sitio deberá contener las siguientes secciones:

    - Fundamentos de Seguridad Informática

[2] Es un formato estandarizado para compartir encabezados y/o descripciones completas de las notas de periódicos en línea, portales, anuncios clasificados, blogs (blogs) o incluso cualquier otra información disponible en un sitio Web.

- Manuales
- Herramientas de Seguridad
- Noticias informativas a través de RSS
- Videos
- Sitios de Interés
- Normas – Estándares

2.4 Revisión y selección de metodología de desarrollo

La metodología de desarrollo es el proceso a seguir sistemáticamente para idear, implementar y mantener un producto software desde que surge la necesidad del producto hasta que se cumple el objetivo por el cual fue creado.

Los ciclos de vida del Software que se revisa son:

- Modelo cascada
- Modelo incremental
- Modelo de desarrollo evolutivo
- Modelo espiral

2.4.1 Modelo cascada

Es el enfoque metodológico que ordena rigurosamente las etapas del ciclo de vida del software (figura 2.1), de forma tal que el inicio de cada etapa debe esperar a la finalización de la inmediatamente anterior.

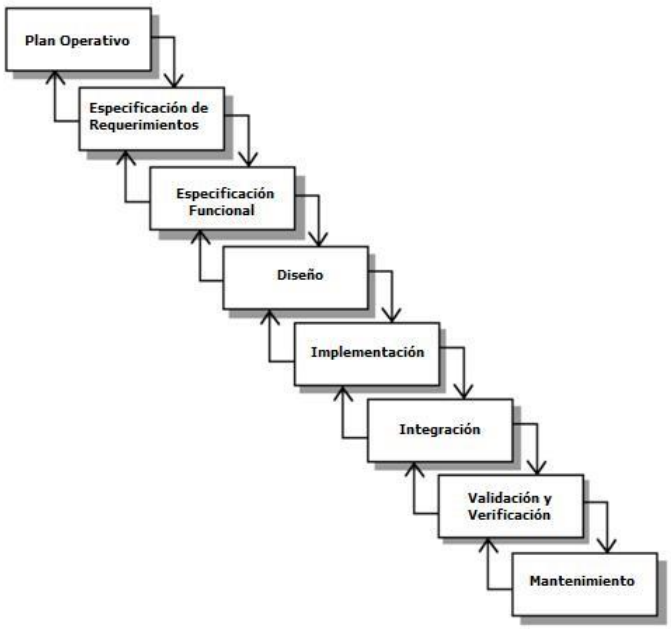


Figura 2.1 Modelo cascada

Ventajas:

- Se tiene todo bien organizado y no se mezclan las fases.
- Es perfecto para proyectos que son rígidos, y además donde se especifiquen muy bien los requerimientos y se conozca muy bien la herramienta a utilizar.

Desventajas:

- Los resultados se visualizan hasta que se encuentra en las etapas finales del ciclo, por lo que cualquier error detectado ocasiona un retraso y aumenta el costo del desarrollo en función del tiempo que insume la corrección de éstos.
- Este modelo es muy restrictivo y no permite movilizarse entre fases.

2.4.2 Modelo incremental

Es un proceso de desarrollo de software, creado en respuesta a las debilidades del modelo tradicional de cascada (figura 2.2).

Este modelo de ciclo de vida se basa en la filosofía de construir incrementando las funcionalidades del programa.

Se realiza construyendo por módulos que cumplen las diferentes funciones del sistema. Este ciclo de vida facilita las tarea de desarrollo permitiendo a cada miembro del equipo desarrollar un módulo particular en el caso de que el proyecto sea realizado por un grupo de programadores, de esta forma al final de cada ciclo se entrega una versión al usuario que contendrá una nueva funcionalidad. Este ciclo de vida permite realizar entregas al usuario antes de terminar el proyecto.

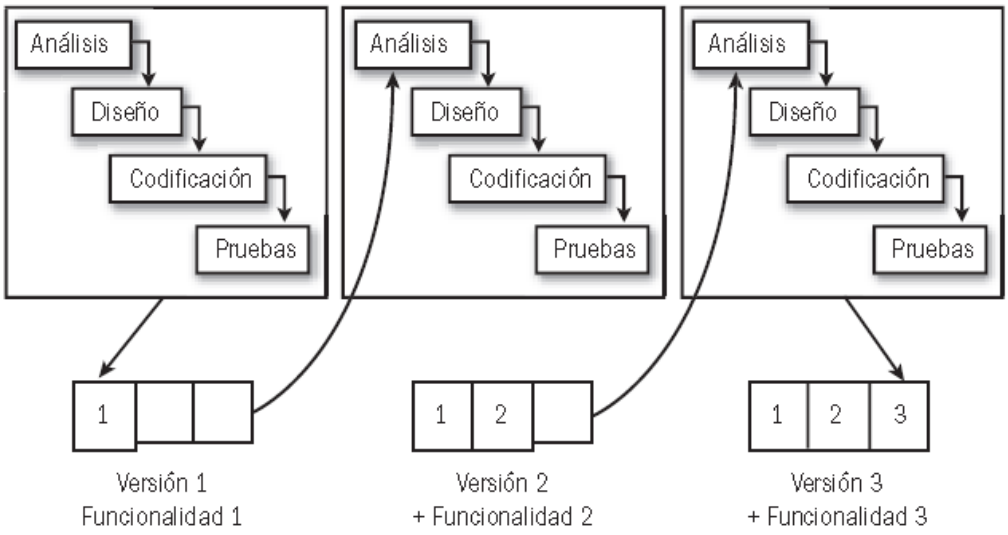


Figura 2.2 Modelo incremental

Ventajas:

- Reduce los riesgos al generar sistemas pequeños, ya que construir un sistema pequeño siempre es menos riesgoso que construir un sistema grande.
- Al desarrollarse independientemente las funcionalidades, es más fácil cambiar los requerimientos del usuario.
- Si se detecta un error grave, sólo se desecha la última iteración.
- No es necesario disponer de los requerimientos de todas las funcionalidades en el comenzó del proyecto

Desventajas:

- Debido a la interacción con los usuarios finales, puede llevar a que los avances sean extremadamente lentos.

2.4.3 Modelo desarrollo evolutivo

Construye una serie de grandes versiones sucesivas de un producto, sin embargo, asume que los requerimientos no son completamente conocidos al inicio del proyecto. Los requerimientos son cuidadosamente examinados, y sólo esos que son bien comprendidos son seleccionados para el primer incremento. Los desarrolladores construyen una implementación parcial del sistema que recibe sólo estos requerimientos.

El sistema es entonces desarrollado, los usuarios lo usan, y proveen realimentación a los desarrolladores. Basada en esta realimentación, la especificación de requerimientos es actualizada, y una segunda versión del producto es desarrollada y desplegada. El proceso se repite indefinidamente (figura 2.3).

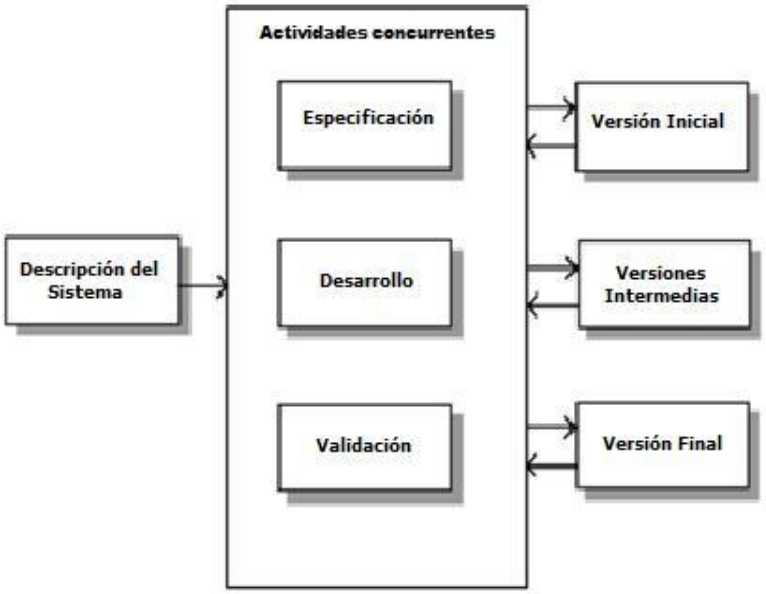


Figura 2.3 Modelo desarrollo evolutivo

Ventajas:

- Este modelo es muy útil cuando desconocemos la mayoría de los requerimientos iniciales, o estos requerimientos no están completos.
- Ofrece un mejor enfoque cuando el responsable del desarrollo del software está inseguro de la eficacia de un algoritmo, de la adaptabilidad de un sistema operativo o de la forma que debería tomar la interacción humano-máquina.

Desventajas:

- El desarrollo de software en forma evolutiva requiere un especial cuidado en la manipulación de documentos, programas, datos de test, etc. desarrollados para distintas versiones del software.
- Este modelo se encuentra con el problema de que en cada versión tiene que evaluar los requerimientos, el desarrollo y la evaluación para la obtención de una nueva versión.

2.4.4 Modelo espiral

El modelo se basa en una serie de ciclos repetitivos para ir obteniendo madurez en el producto final. Este modelo tiene más en cuenta el concepto de riesgo que aparece debido a las incertidumbres e ignorancias de los requerimientos proporcionados al principio del proyecto o que surgirán durante el desarrollo. A medida de que el ciclo se cumple el avance del espiral, (figura 2.4), se van obteniendo prototipos sucesivos que van ganando la satisfacción del cliente o usuario.

A menudo, la fuente de incertidumbre es el propio cliente o usuario, que en la mayoría de las oportunidades no sabe con perfección todas las funcionalidades que debe tener el producto.

Este modelo tiene cuatro etapas:

1. **Planificación:** Relevamiento de requerimientos iniciales después de una iteración.

2. **Análisis de riesgos:** De acuerdo al relevamiento de requerimientos se decide si se continúa con el desarrollo.

3. **Implementación (Ingeniería):** Desarrollo de un prototipo basado en los requerimientos.

4. **Evaluación:** El cliente evalúa el prototipo, si es de su conformidad, termina el proyecto. En caso contrario, se incluye nuevos requerimientos solicitados por el usuario en la siguiente iteración.

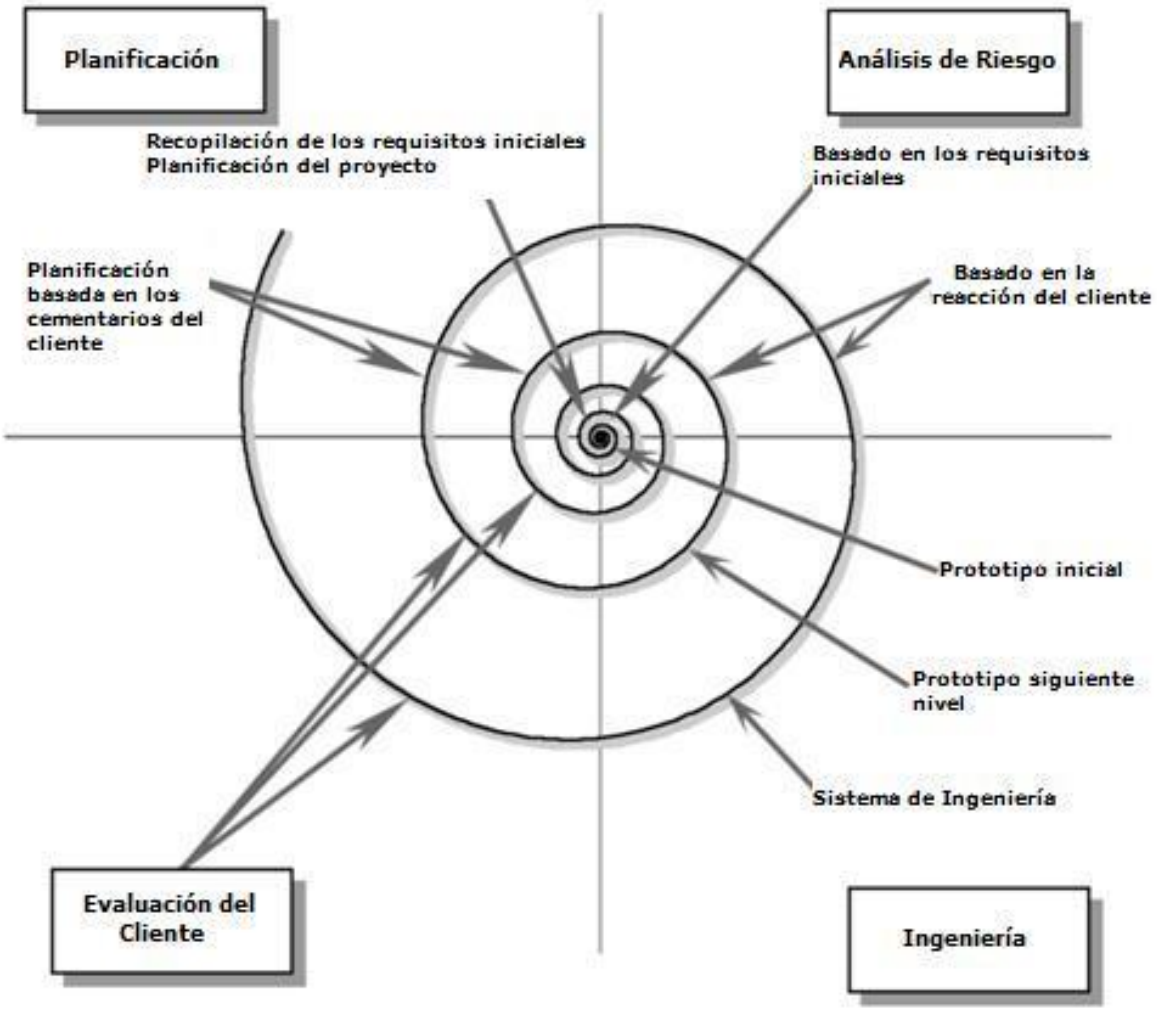


Figura 2.4 Modelo espiral

Ventajas:

- Se puede comenzar el proyecto con un alto grado de incertidumbre
- Se tiene un bajo riesgo de retraso en caso de detección de errores, ya que se pueden solucionar en la próxima rama del espiral
- Este ciclo de vida no es rígido ni estático
- Es un modelo adecuado para grandes proyectos donde no es posible contar con todos los requerimientos desde el comienzo

Desventajas:

- El costo temporal que suma cada vuelta del espiral
- Dificultad para evaluar los riesgos y la necesidad de la presencia o la comunicación continua con el cliente o usuario
- Genera mucho tiempo en el desarrollo del sistema
- Requiere experiencia en la identificación de riesgo

2.4.5 Selección de metodología de desarrollo

Al revisar los distintos ciclos de vida de software mediante la tabla 2.1 y relacionarlos con los recursos y tiempo disponibles podemos ver que el que se adapta más a nuestras necesidades es el modelo incremental. Debido a que se tienen claro desde un principio los requerimientos y objetivos del portal, se podrá dividir por módulos y generar pequeños sistemas con los cuales el usuario pueda tener interacción con el sitio y así tener una realimentación y mejorar el portal.

Tabla 2.1 Comparación de los modelos

Características o necesidades	Modelo cascada	Modelo incremental	Modelo desarrollo evolutivo	Modelo espiral
Conocer los requerimientos	No completamente	Si	No completamente	No completamente
Facilidad de moverse entre fases	No	Si	Si	Si
Facilidad de hacer cambios entre fases	No	Si	Si	Si
Facilidad de proporcionar mantenimiento	No	Si	Si	Si
Puede interactuar el usuario con el proyecto antes de finalizar	No	Si	Si	Si
Requiere habilidades especiales	No	No	Si	Si

Además de que este modelo no necesita de alguna habilidad especial en cuanto a la identificación de riesgos como es el caso del modelo evolutivo y en espiral, pero que si el sistema a desarrollar fuera un proyecto muy largo y rígido serian modelos que se adecuarían muy bien.

Al utilizar el modelo incremental no es necesario tener el portal terminado para que pueda ser probado y evaluado por los usuarios, ya que se planea realizarlo por módulos y de esta forma permitir la interacción del portal con los usuarios y así obtener una evaluación del portal en cortos períodos de tiempo, donde el usuario proporcione una crítica constructiva y así solucionar problemas que se hayan presentado y poder continuar con la mejora del portal. De esta forma cuando se finalice el proyecto y que se realicen las pruebas finales, los ajustes que se tengan que realizar sean mínimos y el portal esté disponible en su totalidad en el tiempo programado.

2.5 Diseño conceptual

El objetivo de esta fase es definir un esquema de organización, funcionamiento y navegación del sitio, centrándose únicamente en la arquitectura de la información, ya que posteriormente se verá la apariencia que tendrá el portal. Debido a que el portal de SI proporcionará contenidos con texto, videos, herramientas y además de un foro, los usuarios pueden optar por buscar información específica o ir a determinada sección del sitio, sin embargo se debe organizar toda la información en una estructura que permita su navegación de manera ordenada y jerárquica, ya que de esta forma el usuario se ubicará rápidamente en el contenido y dimensión del sitio.

Antes de organizar una navegación debemos establecer las secciones que contendrá el sitio (tabla 2.2).

Tabla 2.2. Secciones del sitio

Sección	Contenido	Tipo
Fundamentos de Seguridad	Conceptos teóricos sobre SI	Conocimiento
Documentos de descarga	Documentos informativos	Conocimiento
Herramientas de SI	Ofrecer software o aplicaciones de SI	Práctico
Noticias	Informar a los usuarios sobre temas de SI	Informativa
Videos	Proporcionar ayuda visual a los usuarios	Conocimiento
Sitios de Interés	Proporcionar ligas a otros portales que traten temas de SI	Informativa y de conocimiento

Normas – Estándares	Proporcionar al usuario las diferentes normas y estándares que existen en materia de SI	Conocimiento

Como se puede observar en la tabla 2.2, el portal de SI contará con 4 tipos de contenido, que son el de Conocimiento, Práctico, Interacción e Informativo, donde el de Conocimiento se refiere a las secciones que proporcionarán información teórica donde su finalidad será transmitir al usuario conocimientos teóricos sobre SI, el Práctico se refiere a las secciones donde se pondrá a disposición del usuario material de ayuda para realizar las prácticas de SI, el de Interacción es lo correspondiente a los foros donde el usuario podrá interactuar con otras personas donde se puedan tratar temas de SI y el Informativo es donde se pretende mantener informado al usuarios de los últimos acontecimientos de SI.

Una vez definidas las secciones que contendrá el sitio, podemos establecer los menús que estarán en el sitio, como son:

1. Un menú con información sobre el entorno del sitio (webmaster, políticas de uso de la información, mapa del sitio, etc.).

2. Un menú con los servicios o herramientas (buscador, campos de acceso a secciones especiales para miembros de la página, chat, foros, etc.).

3. Un menú para navegación general del contenido.

Los cuales se colocarán estratégicamente.

Por lo que podemos ver que en el portal de SI existirán conjuntos de páginas interrelacionadas por enlaces unidireccionales y cada una de las páginas puede contener sub-elementos con entidad propia, contenidos multimedia y herramientas interactivas. Por lo que es importante ver el tipo de estructura que se utilizará.

La estructura del sitio web se refiere a su topología, esto es, las conexiones y relaciones entre páginas.

Un sitio web puede encontrarse estructurado de forma muy diversa, solapar diferentes tipos de estructuras y contener subestructuras diferentes a la estructura general.

A continuación se exponen las estructuras más comunes.

2.5.1 Estructuras secuenciales

Las páginas se encuentran interrelacionadas de forma lineal (figura 2.5). Esta estructura se utiliza en tareas de navegación o interacción en las que es necesario que el usuario complete cada uno de los pasos ordenadamente (carrito de compra, registro como usuario,...) o para la segmentación de bloques de información de naturaleza secuencial (artículos, comics, diapositivas, etc.).

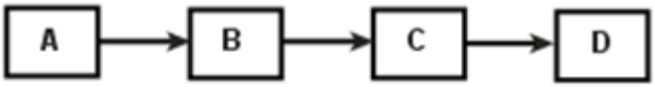


Figura 2.5 Estructura secuencial

Se trata de un tipo de estructura muy sencilla por lo que no provoca desorientación alguna al usuario en la navegación.

2.5.2 Estructuras hipertextuales

El hipertexto es la base sobre la que se asienta la Web. En una estructura hipertextual las páginas se enlazan por similitud o relación directa entre los contenidos, permitiendo al usuario que se encuentra visualizando una página 'saltar' hacia otras que le puedan interesar por contener información relacionada (figura 2.6).

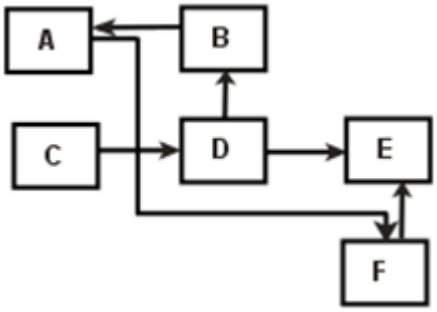


Figura 2.6 Estructura hipertextual

Este tipo de estructura, si bien ofrece mayor libertad y dinamismo a la navegación puede ocasionar desorientación, provocando que el usuario se sienta 'perdido'.

Además, en este tipo de estructuras hay que tener precaución para que ninguna página quede excesivamente descolgada o de difícil acceso.

2.5.3 Estructuras jerárquicas

Probablemente la jerárquica es la estructura de información más común en sitios web, debido en gran medida a su popularización por grandes portales y directorios temáticos. La organización en forma de árbol, por un lado resulta lo suficientemente flexible y escalable como para posibilitar la organización de grandes cantidades de páginas, y por otro resulta muy orientativa para el usuario en su navegación (figura 2.7).

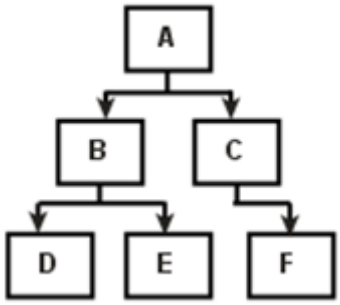


Figura 2.7 Estructura jerárquica

Normalmente, las estructuras jerárquicas se utilizan junto a las hipertextuales, permitiendo al usuario una vez llegado a una página de una rama 'saltar' hacia páginas de otras ramas pero relacionadas temáticamente con la página actual.

En este tipo de estructuras hay que intentar mantener un equilibrio entre ancho y profundidad de la jerarquía. Jerarquías muy profundas pueden provocar que las páginas finales queden muy distanciadas de la página origen, y por tanto de difícil recuperación o concurrencia. Por otro lado, jerarquías muy anchas pueden desorientar y confundir al usuario al ofrecer demasiadas opciones de navegación desde una misma página.

2.5.4 Estructura de la información del portal

La estructura del sitio albergará las tres estructuras mencionadas, la estructura secuencial se utilizará cuando los usuarios revisen un tema en específico y este les permita continuar al apartado siguiente, mientras que la estructura hipertextual será utilizada cuando navegando por los diversos contenidos del sitio existan ligas hacia herramientas y videos, y la estructura jerárquica se encontraría en la mayoría de las páginas que generarían las diferentes secciones.

2.6 Herramientas de desarrollo web

Actualmente existen diferentes lenguajes de programación para desarrollar en la web, estos han ido surgiendo debido a las tendencias y necesidades de las plataformas. A continuación se muestran los lenguajes más conocidos, así como sus ventajas y desventajas.

2.6.1 Lenguaje XHTML

XHTML (eXtensible Hyper Text Markup Language) es el lenguaje de marca creado para sustituir al lenguaje HTML (Hyper Text Markup Language). Desarrollado por el World Wide Web Consortium (W3C). Su objetivo es lograr páginas web donde la información y la forma de presentarla estén claramente separadas.

XHTML sirve únicamente para transmitir la información que contiene un documento, dejando el aspecto y el diseño para las hojas de estilos (CSS), y la interactividad y funcionalidad para JavaScript.

El lenguaje XHTML se basa en el uso de etiquetas también llamadas marcas, directivas o comandos (tags). Los archivos pueden tener las extensiones (htm, html) (Orós, 2007).

Sintaxis:

<html> (Inicio del documento HTML)
<head>
(Cabecera)
</head>
<body>
(Cuerpo)
</body>
</html>
  Negrita
  Definir párrafo
<etiqueta> Apertura de la etiqueta
</etiqueta> Cierre de la etiqueta

Ventajas:

- Sencillo que permite describir hipertexto.
- Texto presentado de forma estructurada y agradable.
- Archivos pequeños.
- Despliegue rápido.
- Lenguaje de fácil aprendizaje.

Desventajas:

- Lenguaje estático.
- La interpretación de cada navegador puede ser diferente, por lo que algunas funciones no podrán visualizarse en todos los navegadores.
- Guarda muchas etiquetas que pueden convertirse en "basura" y dificultan la corrección.
- El diseño es más lento.
- Las etiquetas son muy limitadas.

2.6.2 Lenguaje Javascript

Este es un lenguaje interpretado, no requiere compilación. Fue creado por Brendan Eich en la empresa Netscape Communications. Utilizado principalmente en páginas web. Es similar a Java, aunque no es un lenguaje orientado a objetos, el mismo no dispone de herencias. La mayoría de los navegadores en sus últimas versiones interpretan código Javascript, sobre todo en aplicaciones AJAX.

Sintaxis:

<script type="text/javascript"> ... </script>

Ventajas:

- Lenguaje de scripting seguro y fiable.
- Los script tienen capacidades limitadas, por razones de seguridad.
- El código Javascript se ejecuta en el cliente.

Desventajas:

- Código visible por cualquier usuario.
- El código debe descargarse completamente.
- Puede poner en riesgo la seguridad del sitio, con el actual problema llamado XSS (significa en inglés Cross Site Scripting renombrado a XSS por su similitud con las hojas de estilo CSS).

2.6.3 Lenguaje PHP

PHP es el lenguaje de desarrollo Web escrito por y para desarrolladores Web. PHP significa Hypertext Preprocessor. PHP es un lenguaje de script del lado del servidor, nombre usado para crear aplicaciones Web en combinación con un servidor Web, como Apache. PHP también se puede utilizar para crear scripts de línea de comando semejantes a scripts Perl o Shell, pero dicho uso es menos común que el uso de PHP como lenguaje Web (Suehring, Converse, & Park, 2009).

PHP es un lenguaje de script interpretado en el lado del servidor utilizado para la generación de páginas web dinámicas, embebidas en páginas HTML y ejecutadas en el

servidor. PHP no necesita ser compilado para ejecutarse. Los archivos cuentan con la extensión (php).

Sintaxis:

```
<?php
$mensaje = "Hola";
echo $mensaje;
?>
```

Ventajas:

- Se caracteriza por ser un lenguaje muy rápido
- Soporta en cierta medida la orientación a objeto. Clases y herencia
- Es un lenguaje multiplataforma: Linux, Windows, entre otros
- Capacidad de conexión con la mayoría de los manejadores de base de datos: MySQL, PostgreSQL, Oracle, MS SQL Server, entre otras.
- Capacidad de expandir su potencial utilizando módulos
- Posee documentación en su página oficial la cual incluye descripción y ejemplos de cada una de sus funciones
- Es libre, por lo que se presenta como una alternativa de fácil acceso para todos
- Incluye gran cantidad de funciones

Desventajas:

- Todo el trabajo lo realiza el servidor, por lo tanto puede ser más ineficiente a medida que las solicitudes aumenten de número.
- La legibilidad del código puede verse afectada al mezclar sentencias HTML y PHP.
- La programación orientada a objetos es aún muy deficiente para aplicaciones grandes.

2.6.4 Lenguaje ASP

Active Server Pages (ASP), es una tecnología propietaria de Microsoft. Se trata básicamente de un lenguaje de tratamiento de textos (scripts), basado en Basic, y que se denomina VBScript (Visual Basic Script). Se utiliza casi exclusivamente en los servidores Web de Microsoft (Internet Information Server y Personal Web Server). Los scripts ASP se ejecutan, por lo tanto, en el servidor y puede utilizarse conjuntamente con HTML y Javascript para realizar tareas interactivas y en tiempo real con el cliente. Los archivos cuentan con la extensión (asp).

Sintaxis:

```
<% %>
```

Ventajas:

- Usa Visual Basic Script, siendo fácil para los usuarios
- Comunicación óptima con SQL Server
- Soporta el lenguaje JScript (Javascript de Microsoft)

Desventajas:

- Solo funciona en plataforma Windows
- Tecnología propietaria
- El programador no lleva el control de las aplicaciones porque ya están prediseñadas

2.6.5 Lenguaje ASP.NET

Este es un lenguaje comercializado por Microsoft, y usado por programadores para desarrollar entre otras funciones, sitios web. ASP.NET es el sucesor de la tecnología ASP, fue lanzada al mercado mediante una estrategia de mercado denominada .NET.

El ASP.NET fue desarrollado para resolver las limitantes que brindaba su antecesor ASP. Creado para desarrollar web sencillas o grandes aplicaciones. Para el desarrollo de ASP.NET se puede utilizar C#, VB.NET o J#. Los archivos cuentan con la extensión (aspx). Para su funcionamiento de las páginas se necesita tener instalado IIS (Internet Information Server) con el Framework.NET.

Ventajas:

- Completamente orientado a objetos.
- Controles de usuario y personalizados.
- División entre la capa de aplicación o diseño y el código.
- Facilita el mantenimiento de grandes aplicaciones.
- Incremento de velocidad de respuesta del servidor.
- Mayor velocidad *que ASP*.
- Mayor seguridad *que ASP*.

Desventajas:

- Mayor consumo de recursos que ASP
- Solo funciona en Sistema Operativo Windows
- Hay que solicitar licencia.

2.6.6 Lenguaje JSP

Es un lenguaje para la creación de sitios web dinámicos, acrónimo de Java Server Pages. Está orientado a desarrollar páginas web en Java. JSP es un lenguaje multiplataforma. Creado para ejecutarse del lado del servidor.

JSP fue desarrollado por Sun Microsystems. Comparte ventajas similares a las de ASP.NET, desarrollado para la creación de aplicaciones web potentes. Posee un motor de páginas basado en los servlets de Java. Para su funcionamiento se necesita tener instalado un servidor Tomcat.

Sintaxis:

<%= new java.util.Date() %>

Características:

- Código separado de la lógica del programa.
- Las páginas son compiladas en la primera petición.
- Permite separar la parte dinámica de la estática en las páginas web.
- Los archivos se encuentran con la extensión (jsp).
- El código JSP puede ser incrustado en código HTML.

Elementos de JSP:

Los elementos que pueden ser insertados en las páginas JSP son los siguientes:

- *Código:* se puede incrustar código "Java".
- *Directivas:* permite controlar parámetros del servlet.
- *Acciones:* permite alterar el flujo normal de ejecución de una página.

Ventajas:

- Ejecución rápida del servlets.
- Crear páginas del lado del servidor.
- Multiplataforma.
- Código bien estructurado.
- Integridad con los módulos de Java.
- La parte dinámica está escrita en Java.
- Permite la utilización de servlets.

Desventajas:

- Difícil para los que no conozcan Java
- Poco práctico para pequeños proyectos
- Tiempos de desarrollo mayores que con otras tecnologías

2.6.7 Lenguaje Python

Es un lenguaje de programación creado en el año 1990 por Guido van Rossum, es el sucesor del lenguaje de programación ABC. Permite la creación de todo tipo de programas incluyendo los sitios web.

Su código no necesita ser compilado, por lo que se llama que el código es interpretado. Es un lenguaje de programación multiparadigma, lo cual fuerza a que los programadores adopten por un estilo de programación particular:

- Programación orientada a objetos.
- Programación estructurada.
- Programación funcional.
- Programación orientada a aspectos.

Sintaxis:

Ejemplo de una clase en Phyton:

```
def dibujar_muneco(opcion):
   if opcion == 1:
      C.create_line(580, 150, 580, 320, width=4, fill="blue")
      C.create_oval(510, 150, 560, 200, width=2, fill='PeachPuff')
```

Ventajas:

- Libre y fuente abierta
- Lenguaje de propósito general
- Gran cantidad de funciones y librerías
- Sencillo y rápido de programar
- Multiplataforma
- Licencia de código abierto (Opensource)
- Orientado a Objetos
- Portable

Desventajas:

- Su desventaja primordial es la velocidad, debido a la necesidad de traducir el programa mientras se ejecuta. Este aspecto se debe evaluar a fondo al crear software con este tipo lenguajes, ya que se debe equilibrar la portabilidad con la velocidad que se está sacrificando.

2.6.8 Lenguaje Ruby

Es un lenguaje interpretado de muy alto nivel y orientado a objetos. Desarrollado por el programador japonés Yukihiro Matsumoto. Su sintaxis está inspirada en Perl, Smalltalk, Eiffel y Lisp. Es distribuido bajo licencia de software libre (Opensource).

Sintaxis:

```
puts "hola"
```

Características:

- Existe diferencia entre mayúsculas y minúsculas.
- Múltiples expresiones por líneas, separadas por punto y coma ";".
- Dispone de manejo de excepciones.
- Ruby puede cargar librerías de extensiones dinámicamente si el Sistema Operativo lo permite.
- Portátil.

Ventajas:

- Permite desarrollar soluciones a bajo Costo.
- Software libre.
- Multiplataforma.

Desventajas:

- La desventaja del intérprete es su velocidad ya que debe pasar por varias etapas o capas, para que se comprendan todas sus instrucciones.

2.6.9 CSS

Las hojas de estilo en cascada, CSS o Cascading Style Sheet, se convirtieron en una recomendación del W3C (World Wide Web Consortium) en diciembre de 1996. Las hojas de estilo permiten generar un estilo patrón para todo el resto de los documentos de una web, con el consiguiente ahorro de tiempo en diseño y mantenimiento.

Su misión es definir la apariencia y el estilo de sus elementos.

Sintaxis:

```
<style type= "txt/css">
body{
        background-color: #33FF66;
        background-position: 0px;
        cursor: hand;
}
```

2.6.10 XML

El XML (eXtensible Markup Language) es un lenguaje usado para estructurar información en un documento o en general en cualquier fichero que contenga texto, como por ejemplo ficheros de configuración de un programa o una tabla de datos. Se convirtió en estándar de transmisión de información estructurada en la web.

```
<?xml version='1.0' encoding="iso-8859-1" ?>
<documento>
<encabezado>
        <titulo> …. </titulo>
        <autor> …. </autor>
</encabezado>
<texto>
```

2.6.11 AJAX

AJAX (Asynchronous JavaScript And XML), es una combinación de JavaScript, que trabaja del lado del cliente, y de lenguajes que procesan la información en el servidor y la entregan como una cadena de texto o en un archivo XML, lo que proporciona una gran posibilidad de uso a los datos.

A la letra 'A' del acrónimo AJAX le corresponde la palabra Asynchronous (asíncrono). Al hacer las peticiones de esta manera, es decir de forma asíncrona, podemos mostrar la información que el servidor retorna, sólo en las secciones de la página en donde nos interesa mostrarla, sin necesidad de actualizarla por completo.

AJAX permite desarrollar aplicaciones web mucho más atractivas para el usuario, puesto que son más ágiles y de respuesta inmediata.

2.6.12 Lenguaje de desarrollo seleccionado

De acuerdo al análisis anterior los lenguajes de desarrollo web a utilizar para el portal de Seguridad Informática son:

- XHTML debido a que toda página web contiene etiquetas HTML, y XHTML es estricto, debido a que las etiquetas y propiedades serán escritas debido a que deben seguirse reglas en la apertura y cierre de etiquetas, así como en la utilización de propiedades. XHTML nos permite trabajar con estándares, atenerse a ellos y realizar páginas más simples, con código más legible para realizar más fácil su modificación y actualización en un futuro.

- CSS u hojas de estilo que permite definir el estilo visual de los diferentes elementos contenidos en la página Web.

- AJAX que permite desarrollar aplicaciones web mucho más atractivas para el usuario, debido a que son más ágiles y de respuesta inmediata, además de sólo recargar secciones de la página en donde nos interesa mostrarla, sin necesidad de actualizarla por completo.

- JavaScript, ya que su uso con aplicaciones AJAX es indispensable para la realización de procedimientos, como es el envío de peticiones de interés al servidor para que se retorne sólo la parte de la página que cambiará y recargue sólo esa parte, en lugar de recargar todo, además de permitir la utilización de la biblioteca jQuery, la cual permite simplificar la manera de interactuar con los documentos HTML, manipular el árbol DOM, manejar eventos, desarrollar animaciones y agregar interacción con la técnica AJAX a páginas web.

- XML, debido a que se trabaja con AJAX, y las aplicaciones AJAX lo utilizan mucho, ya sea mediante la aplicación de sus conceptos al trabajar con el Document Object Model (DOM[3]) en XHTML, para la transmisión de información desde y hacia el servidor o para el almacenamiento de datos.

- PHP como lenguaje de script del lado del servidor, el cual permite la creación de aplicaciones Web en combinación con un servidor Web Apache, así como la generación de páginas web embebidas que simplificarán el diseño y la actualización de las diferentes páginas.

[3] DOM: El Modelo de Objetos del Documento es una interfaz de la plataforma y del lenguaje neutro que permitirá a los programas y scripts acceder y actualizar dinámicamente el contenido, estructura y estilo de los documentos.

2.7 Diseño de contenidos

En el diseño de contenidos se debe contar con un equilibrio que mantenga cierta coherencia informativa, organizativa de comunicación.

La escritura hipertextual se debe realizar de forma diferente a la escritura convencional. A los usuarios no les gusta leer en pantalla, por lo que agradecerán cuanto más les facilitemos dicha tarea. El nuevo medio y sus características obligan a ser concisos, precisos, creativos y estructurados a la hora de redactar. Debemos conocer a quién nos dirigimos y adaptar el lenguaje, tono y vocabulario utilizado al usuario objetivo.

Por lo que debemos tomar en cuenta los siguientes puntos en el diseño y redacción de contenidos:

- ***Seguir una estructura piramidal*:** La parte más importante del mensaje, el núcleo, debe ir al principio.

- ***Permitir una fácil exploración del contenido*:** El lector en entornos Web, antes de empezar a leer, suele explorar visualmente el contenido para comprobar si le interesa.

- ***Un párrafo = una idea*:** Cada párrafo es un objeto informativo. Se deben trasmitir ideas, mensajes... evitando párrafos vacíos o varios mensajes en un mismo párrafo.

- ***Ser conciso y preciso*:** Al lector no le gusta leer en pantalla.

- ***Vocabulario y lenguaje*:** Se debe utilizar el mismo lenguaje del usuario, no el de la empresa o institución. El vocabulario debe ser sencillo y fácilmente comprensible.

- ***Tono*:** Cuanto más familiar y cercano (sin llegar a ser irrespetuoso) sea el tono empleado, más fácil será que el lector preste atención.

- ***Confianza*:** La mejor forma de ganarse la confianza del lector es permitiéndole el diálogo, así como conocer cuanta más información posible acerca del autor.

2.8 Mapa del Sitio

El mapa del sitio se refiere al proceso de crear un "árbol de contenido" en el que se muestre de manera práctica el número de secciones que contendrá el portal de SI y cuántos niveles habrá dentro de cada sección.

Cuando se usa la idea de crear un árbol, se refiere exactamente a generar un diagrama que cuente con un tronco, ramas y hojas, para mostrar las zonas principales, secundarias y contenidos finales que se irán incorporando.

Para generar el árbol de contenidos se debe considerar lo siguiente:

- ***Secciones****:* Se debe intentar que sean las menos posibles, con el fin de concentrar las acciones del usuario en pocas áreas; hay que considerar que cada una de las áreas a integrar en el árbol requerirá de mantenimiento posterior en contenidos, gráfica y funcionalidad, lo que encarecerá el costo final de operación del sitio.

- ***Niveles:*** Es un área específica de los contenidos dentro del sitio, no deben considerarse más de tres niveles de acceso.

- ***Contenidos relacionados:*** se debe considerar que habrá funcionalidades que estén presentes en todo el sitio. Entre ellas se incluyen elementos como Buscador, Preguntas Frecuentes y Formularios de Contacto. Se recomienda que este tipo de elementos quede fuera del "árbol" y "floten" sobre éste, con el fin de indicar que desde todas las páginas habrá enlaces a ellos.

De acuerdo a estos puntos y a los diferentes contenidos de portal de SI, dan como resultado el árbol de contenido que se muestra en la figura 2.8 y el mapa del sitio (figura 2.9).

Figura 2.8 Árbol de contenidos

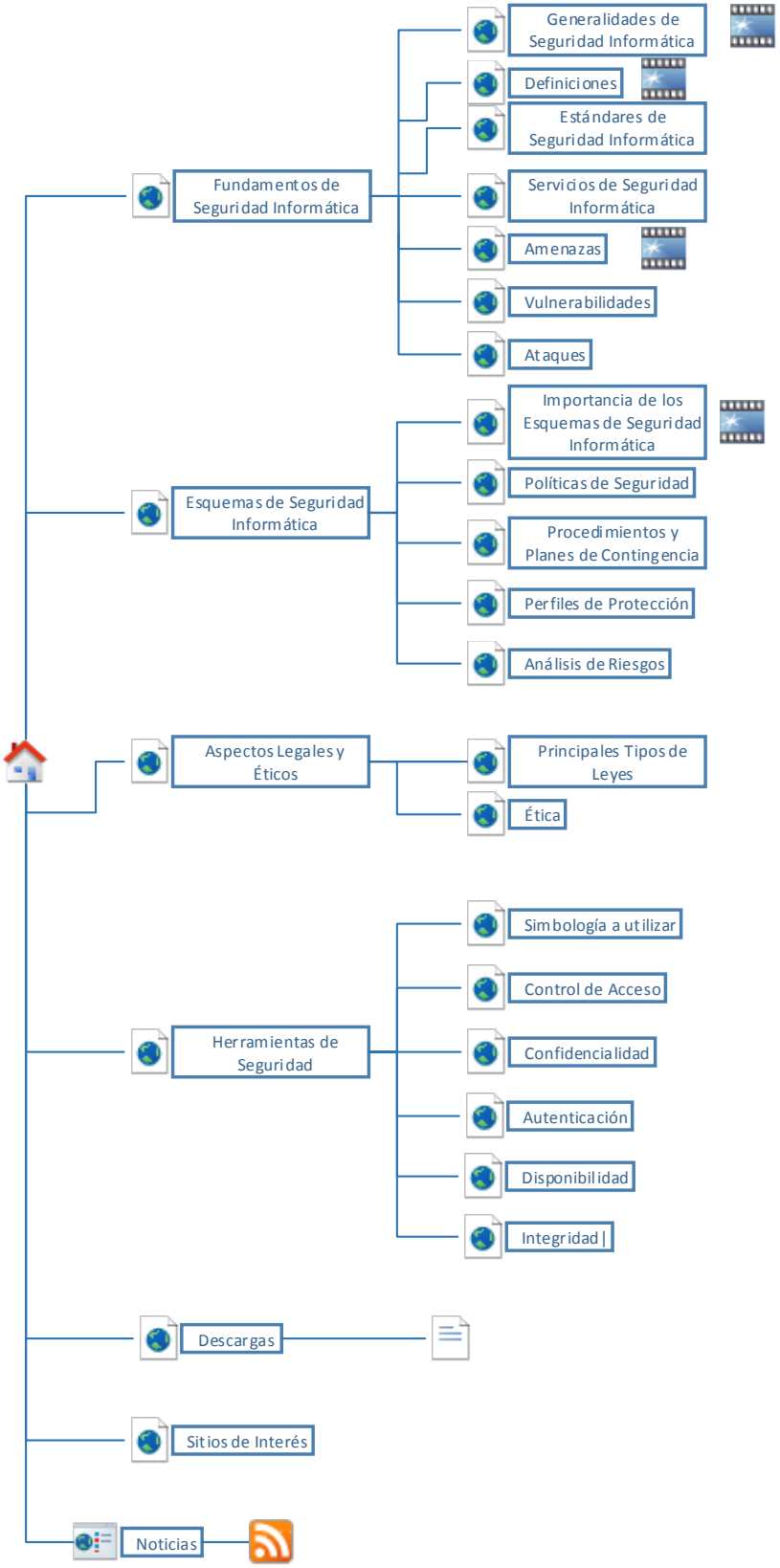


Figura 2.9. Mapa del Sitio

A continuación se detallan cada una de las secciones que contienen páginas internas y que a través de un link o del menú de navegación, el usuario puede acceder a la información de su interés.

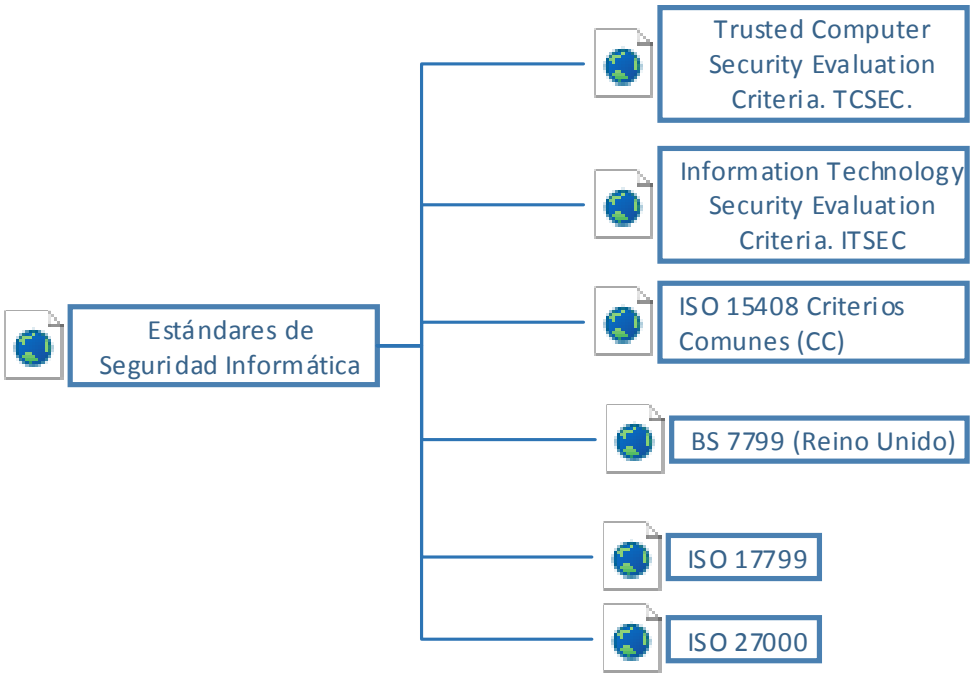


Figura 2.10. Páginas internas de la Sección de Estándares de Seguridad Informática

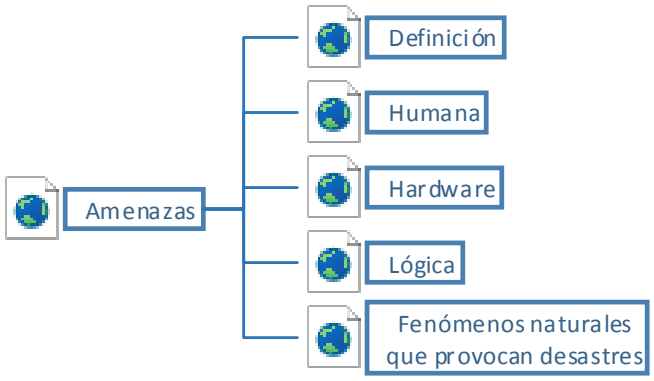


Figura 2.11. Páginas internas de la Sección de Amenazas

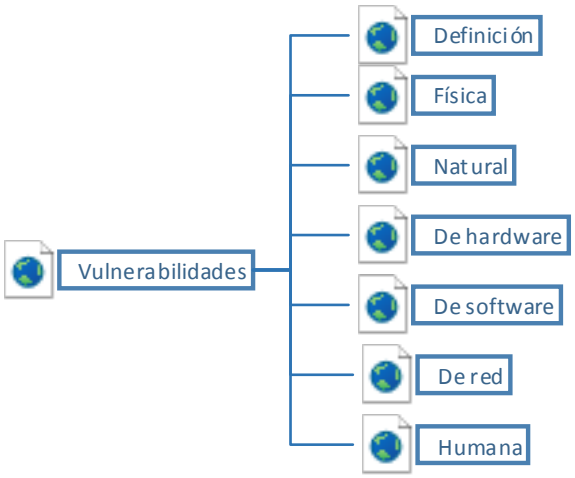


Figura 2.12. Páginas internas de la Sección de Vulnerabilidades

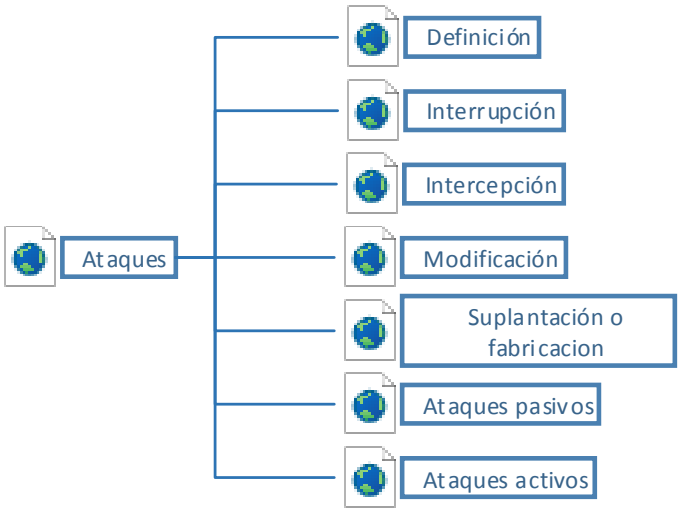


Figura 2.13. Páginas internas de la Sección de Ataques

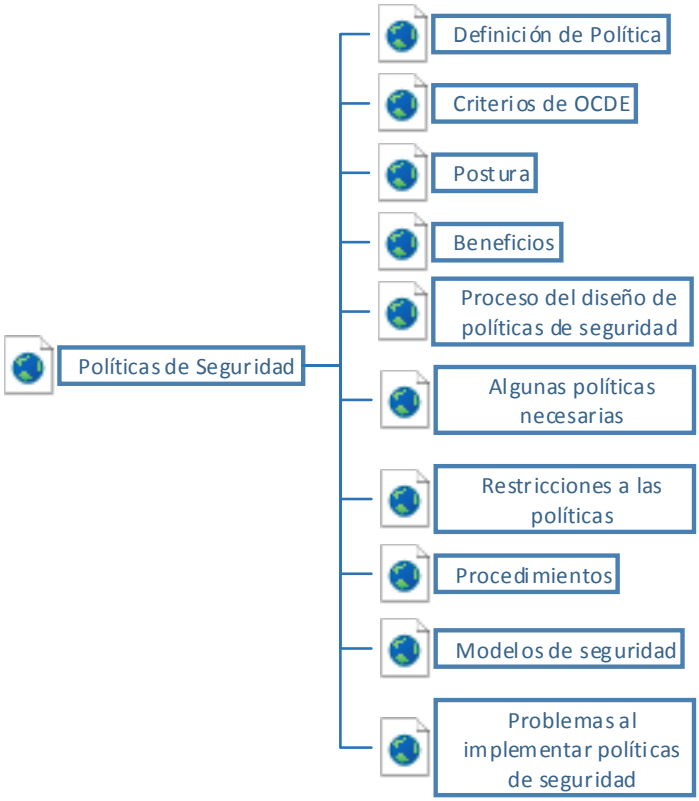


Figura 2.14. Páginas internas de la Sección de Políticas de Seguridad

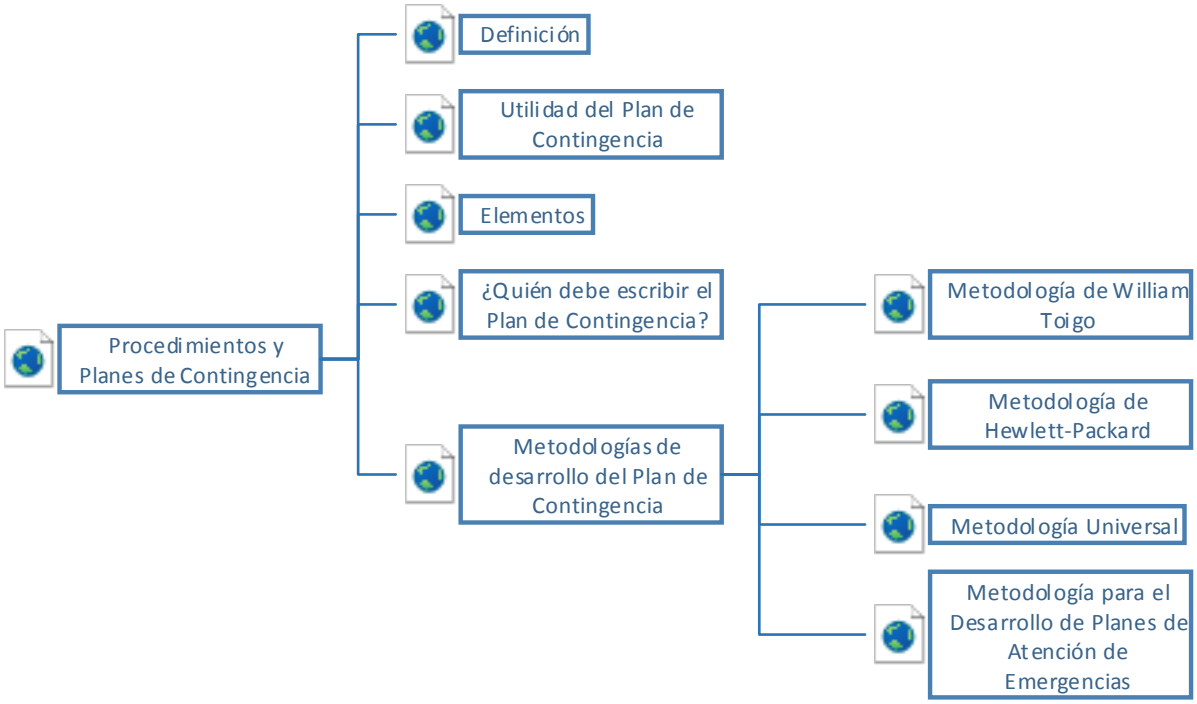


Figura 15. Páginas internas de la Sección de Procedimientos y Planes de Contingencia

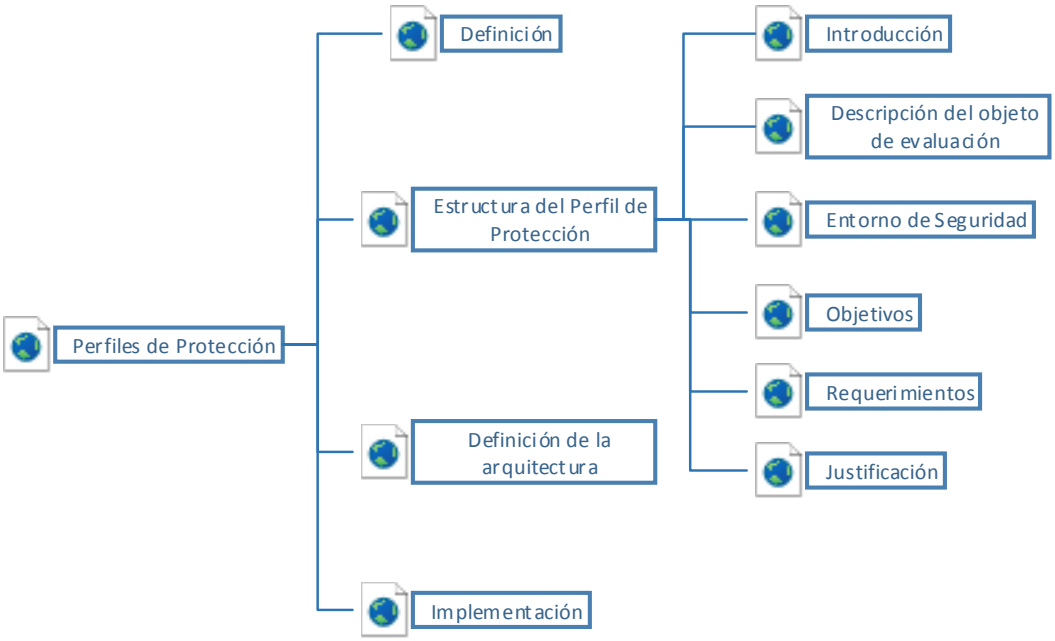


Figura 2.16. Páginas internas de la Sección de Perfiles de Protección

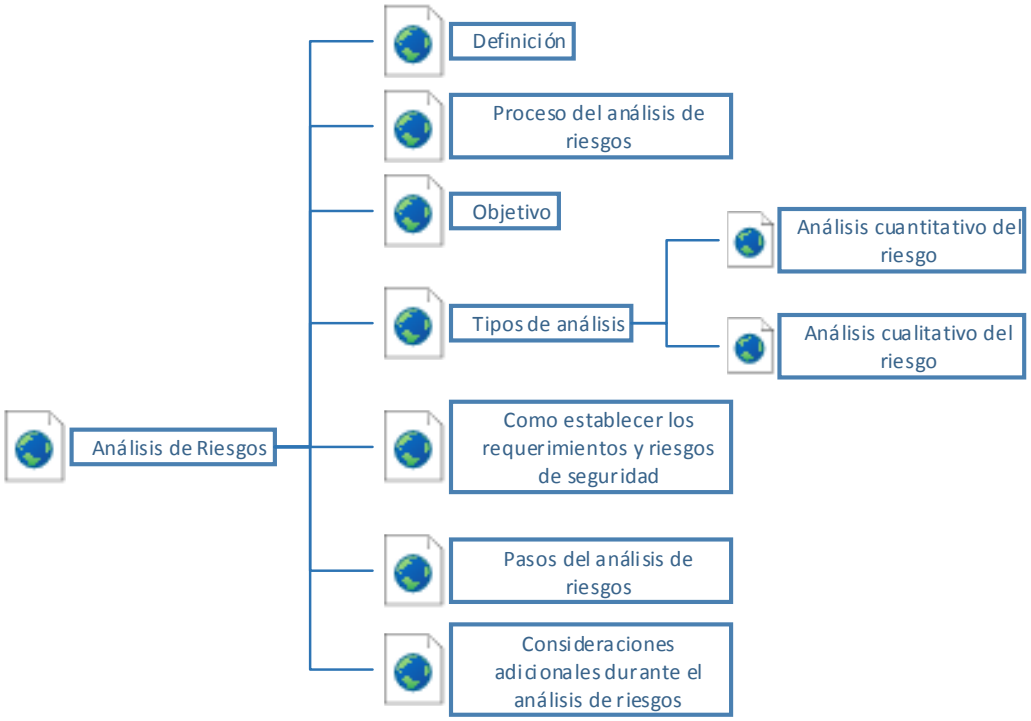


Figura 2.17. Páginas internas de la Sección de Análisis de Riesgos

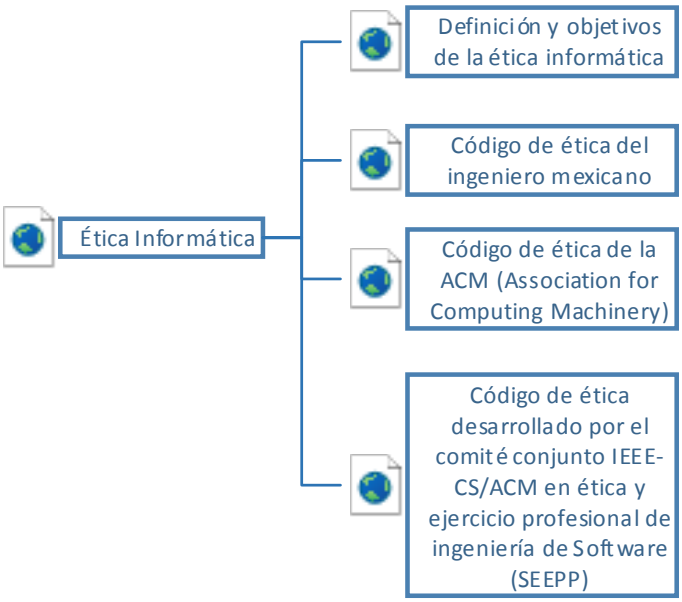


Figura 2.18. Páginas internas de la Sección de Ética Informática

2.8 Diseño visual y definición del estilo

En esta fase se establece el aspecto visual del sitio web, la composición de cada tipo de la página, el aspecto y comportamiento de los elementos de interacción y la presentación de elementos multimedia.

Con el objetivo de evitar la sobrecarga informativa, en el diseño de cada interfaz se debe tener en cuenta el comportamiento del usuario en el barrido visual de la página, distribuyendo los elementos de información y navegación según su importancia en zonas de mayor o menor jerarquía visual, por ejemplo, las zonas superiores de la interfaz poseen más jerarquía visual que las inferiores.

Además de la posición de cada elemento en la interfaz, existen otras técnicas para jerarquizar información como son: uso del tamaño y espacio ocupado por cada elemento para otorgarle importancia en la jerarquía visual, utilización del contraste de color para discriminar y distribuir información, uso de efectos tipográficos para enfatizar contenidos, rotura de la simetría y uso de efectos de relieve / profundidad para resaltar elementos, etc.

Otro aspecto importante en el diseño visual del sitio es la accesibilidad. En el uso de colores, por ejemplo, se debe ofrecer suficiente contraste entre texto y fondo para no dificultar la lectura, e igualmente seleccionar combinaciones de colores teniendo siempre en cuenta las discapacidades visuales en la percepción del color que pudieran presentar nuestros usuarios.

2.8.1 Color y tipografía

Utilizaremos los colores representativos de nuestra institución UNAM, para la interfaz gráfica y contenidos, considerando los contrastes en los colores elegidos para asegurar una visualización correcta en todos los navegadores, resoluciones y sistemas operativos, procurando que no dificulte la legibilidad del sitio o genere mucho brillo en la pantalla y permita un contraste armonioso.

A continuación se presentan los colores utilizados para el sitio en código hexadecimal:

Color para títulos de las secciones: #0E0E5A;
Color de títulos: #202ABC;
Color de tipografía: #000;
Color de enlaces: #202ABC;
Color de fondo: #FFFFFF;

Esto permitirá tener siempre presente los colores que debemos utilizar en todos los elementos del sitio.

El tipo de fuente utilizada dentro del contenido del portal de Seguridad Informática, es la correspondiente a la familia Arial, Helvetica, sans-serif, ya que no tienen problemas de visibilidad en los diferentes sistemas operativos.

2.8.2 Resolución

Los monitores de las computadoras al paso del tiempo han cambiado significativamente sus resoluciones, en la figura 2.19 se puede ver una gráfica donde se muestra el porcentaje de uso de las diversas resoluciones.

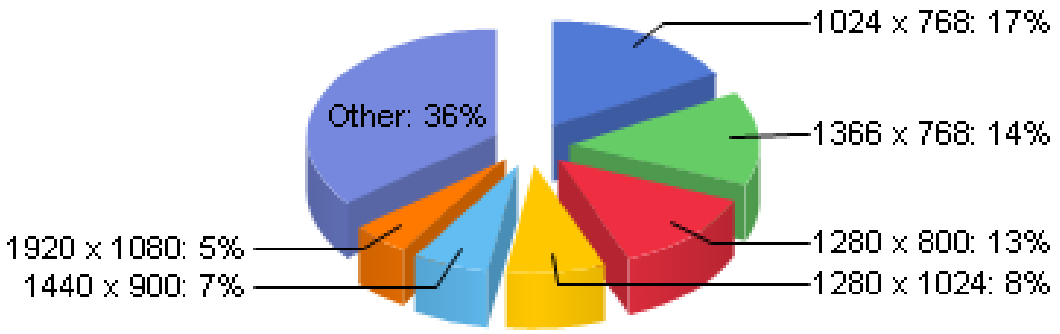


Figura 2.19 Grafica de porcentajes de uso de monitores[4]

[4] **Fuente**: http://www.netmarketshare.com/report.aspx?qprid=17

Por lo que podemos observar que la resolución de 1024 X 768 pixeles es la más utilizada por los usuarios, por lo que el sitio estará optimizado para que la resolución sea lo más similar.

Para que se tenga una distribución uniforme en la página se tiene que considerar:

- Los diferentes elementos que integrarán el portal, como son encabezado, menú, contenido, pie de página, etc.

- Los contenidos deberán estar en una medida de 550 pixeles de altura, para que el contenido esté dentro de la ventana del navegador sin necesidad de usar la barra de desplazamiento vertical.

2.8.3 Esquema de la página

Se debe considerar que las páginas Web pueden contener:

- Menú de Servicios
- Menú de navegación

Por lo tanto para la página Web se propone el esquema mostrado en la figura 2.20

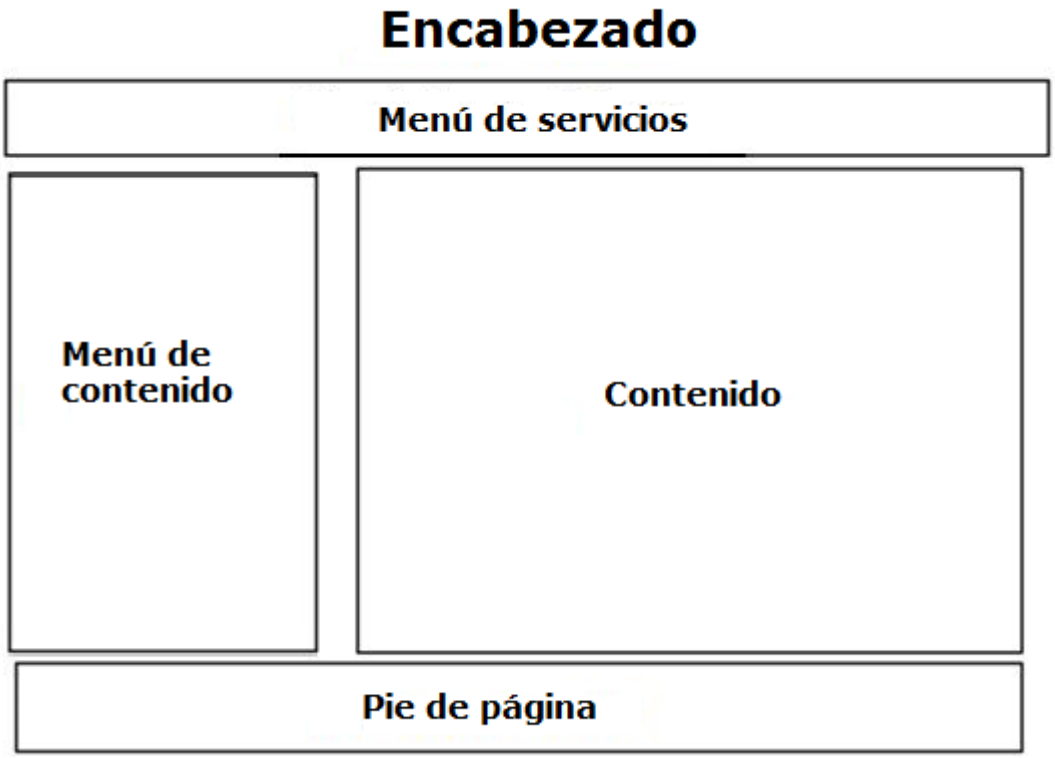


Figura 2.20 Esquema de la página

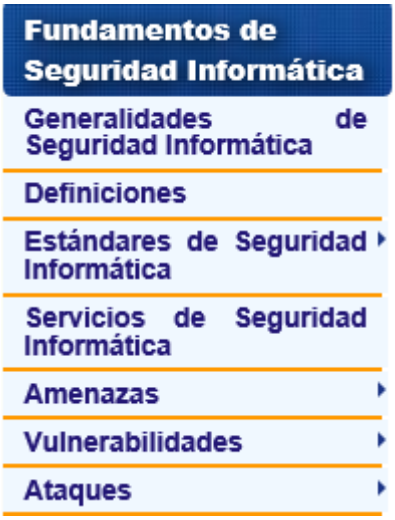
Para aportar una identidad gráfica al sitio y de esta forma crear en el usuario la sensación de recordar claramente el sitio y saber dónde se encuentra situado, por ello se utilizará una sola interfaz gráfica para el portal Web.

Considerando la resolución de 1024 X 728 pixeles y la distribución de los diferentes elementos a emplear dentro del portal de Seguridad Informática, como son encabezado, menú de servicios, menú de navegación y el contenido, dan como resultad los siguientes diseños:

Encabezado:

Menú de servicios:

Menú de contenido:



Pie de página:

Y que en conjunto da como resultado el diseño del portal con dimensiones de 1024 X 806 pixeles, el cual se muestra en la figura 2.21, donde se presentan cada una de las dimensiones de los diferentes elemento que integran al portal de SI.

Figura 2. 21. Esquema final de la página web

Figura 2.22. Esquema final de la página web sin marcas

CAPÍTULO 3

Fundamentos de Seguridad Informática

En este capítulo se dan los fundamentos de Seguridad Informática, iniciándose desde la evolución histórica hasta las tendencias de las tecnologías de la información, continuando con las definiciones básicas, así como de los diferentes estándares existentes y de los diferentes servicios de Seguridad Informática, finalizando con los diferentes tipos de amenazas, vulnerabilidades y ataques existentes.

CAPÍTULO 3

Fundamentos de Seguridad Informática

3.1 Generalidades de Seguridad Informática

3.1.1 Evolución histórica y tendencias de las Tecnologías de la Información

Los avances en las tecnologías de la información, han sido un elemento importante para el progreso de la sociedad, pero antes de comenzar, cabe aclarar qué es lo que entendemos por "tecnologías de la Información (TI)".

Las TI es un término que comprende todas las formas de tecnología empleadas para crear, almacenar, intercambiar, manejar y manipular material digitalizado en sus formas variadas (datos de negocios, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia y otras formas, incluyendo aquellas que aún no se han concebido). Es un término conveniente para incluir tanta a la telefonía como a la tecnología de cómputo en una misma palabra.

Cronología de las Tecnologías de la Información y Comunicación

Fecha	Suceso
1822	**Charles Babbage** diseña y comienza la construcción de lo que dio a conocer como la máquina diferencial para tabular polinomios.
1831	**Joseph Henry** crea un telégrafo eléctrico.
1835	**Samuel Morse** crea el código Morse.
1843	**Samuel Morse** construye la línea Washington-Baltimore de telegrafía eléctrica.
1860	Primer servicio telegráfico intercontinental.
1876	**Alexander Graham Bell** y **Thomas Watson** exhiben un teléfono eléctrico en Boston.
1877	**Thomas Edison** patenta el fonógrafo.
1887	**Heinrich Hertz** demostró que las ondas electromagnéticas pueden ser transmitidas a través del aire.

1889	El ingeniero ruso Alexander Popov inventa la primera antena radioeléctrica.
1896	**Herman Hollerith** fundó la Compañía de Máquinas Tabuladoras, que más tarde la compañía cambiaría al nombre de International Business Machine (IBM).
1904	El británico **John Ambrose Fleming** utiliza una válvula diodo, denominada diodo Fleming, para pasar corriente alterna a corriente directa.
1906	**Lee de Forrest** patenta el tríodo y da nacimiento al primer amplificador electrónico.
1925	**John Logie Baird** transmite la primera señal de televisión.
1931	En el MIT (Instituto Tecnológico de Massachussets), **Vannevar Bush** construye un analizador diferencial, o lo que podría llamarse la primera computadora analógica, que servía para realizar automáticamente algunas de las operaciones elementales.
1936	**Alan Mathison Turing** construyó un modelo formal de computador, la máquina de Turing, y demostró que existían problemas que una máquina no podría resolver.
1938	**Claude Elwood Shannon**, presenta su tesis de licenciatura en el MIT, demostró cómo el álgebra booleana se podía utilizar en el análisis y la síntesis de la conmutación y de los circuitos digitales. Luego, Shanon será recordado como el padre de la "Teoría de la Información".
1941	- El alemán **Konrad Zuse** finaliza su Z3, primera computadora electromecánica digital controlada por un programa completamente funcional. - Desarrollo de la ABC (Atanasoff-Berry Computer) por **John Atanasoff** y **Clifford Berry**, la cual su tarea específica era la resolución de sistemas de ecuaciones lineales.
1943	El norteamericano **John Presper Eckert** diseña el primer programa mecánico y, junto a su amigo **John Williams Mauchly,** comienza la construcción de la primera computadora decimal de propósito general patentada: ENIAC
1946	**John Presper Eckert y John Williams Mauchly** finalizan ENIAC en la Universidad de Pensilvania.
1947	**John Bardee**, **Walter Brattain** y **William B. Shockley** diseñan el transistor, con el cual comienza la substitución de los tubos de vacío, disminuyendo considerablemente el volumen de las máquinas.
1949	Se construye EDVAC (Electronic Delay Storage Automatico Computer) en la Universidad de Manchester. EDVAC, a diferencia de su antecesora ENIAC, era binaria y tuvo el privilegio de almacenar un programa.
1951	La corporación de **Eckert** y **Mauchly** da origen a la primera computadora fabricada comercialmente: UNIVAC I, la primera en utilizar un compilador para que la máquina pudiera interpretar un programa.
1954	Se construye la IBM 650, considerada la primera computadora de producción masiva habiendo 100 de ellas en todo el mundo.

1957	Nace el primer lenguaje de programación de alto nivel desarrollado por la empresa IBM (International Business Machine) llamado FORTRAN.
1959	**Jack S. Kilby** desarrolla en el microchip.
1960	El DEC PDP-1, precursor de las minicomputadoras y fabricada por DEC (Digital Equipment Corporation) introduce el cinescopio, considerado el primer monitor de computadora.
1964	IBM anuncia el lanzamiento del Sistema/360, la primera familia de computadoras compatibles, lo que lleva a que **John Kemeny** y **Thomas Kurtz** desarrollaran, en el Darmouth Collage, el BASIC (Beginners All-purpose Symbolic Instruction Code), siendo el origen de los lenguajes de programación modernos.
1966	**Charles Kao** teoriza sobre la fibra óptica
1971	Nace la primera PC (Personal Computer, en español, Computadora Personal). La **Kenbak 1**, fue fabricada por **John Blankenbaker** de la Kenbak Corporation de Los Angeles. Esta computadora estaba dirigida al mercado educacional y contaba con 256 bytes de memoria RAM.
1973	- Aparece la primera computadora personal comercial, la Altair 8800, diseñada por **Ed Roberts** y **Bill Yates**, fabricada por la empresa MITS (Micro Instrumentation Telemetry Systems). - **Akira Hasegawa** y **Fred Tappert** proponen el uso de señales digitales para transmitir información a través de la fibra óptica.
1976	La primera PC en lograr uso masivo fue la Apple I presentada en este año
1977	Las empresas Apple, Commodore y Tandy distribuyen los primeros ordenadores completamente ensamblados.
1980	**Linn Mollenauer**, **Rogers Stollen,** y **James Gordon** prueban que mediante fibra óptica pueden transmitirse señales.
1981	El fabricante Ericsson lanza el sistema NMT 450 (Nordic Mobile Telephony 450 MHz), el primer sistema del mundo de telefonía móvil.
1981	IBM entra en escena estableciendo un estándar con la primera PC de propósito general distribuida con el sistema operativo PC-DOS (posteriormente MS-DOS).
1989	**Tim Berners-Lee** y **Robert Cailliau** crean el prototipo que se convertirá en la World Wide Web en el CERN.
1991	**Anders Olsson** transmite mediante fibra óptica 4 gigabytes por segundo.
1998	Aparece el primer libro digital.
1999	Nokia y Symbol Technologies crean una asociación conocida como WECA (Wireless Ethernet Compatibility Alliance, Alianza de Compatibilidad Ethernet Inalámbrica).

	- Aparece el Blackberry, desarrollado por la firma canadiense Reasearch in Motion y liberado en 1999, el gadget posibilita la lectura inmediata y ubicua del email y facilita a las personas el mantener a sus empleados digitalmente comunicados.
2001	El iPod, concebido por la luminaria del diseño de Apple, Jonathan Ive, el más grande puede almacenar unas 30,000 canciones, la cual ayudó a revolucionar la industria de la Música
2003	La asociación WECA(Wireless Ethernet Compatibility Alliance) pasó a denominarse Wi-Fi Alliance. El objetivo de la misma fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.
2004	Surge el estándar iSCSI de redes de almacenamiento, que promete beneficios a un rango mucho más amplio: iSCSI o Internet SCSI.
2009	Aparece la tecnología inalámbrica Bluetooth 3.0, con el nuevo sistema será posible alcanzar una velocidad de transmisión de 480 megabytes frente a los 53.3 Mbs de su anterior edición 2.

"Las tecnologías de la información y las comunicaciones tienen, día a día, una mayor presencia en todos los aspectos de la vida laboral y personal, ofreciendo un nuevo espacio de innovación en ámbitos como la industria, los servicios, la salud, la administración, el comercio y la educación".

3.2 Definiciones

Podemos entender como *seguridad* una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible (es decir que el sistema se comporte tal y como se espera que funcione).

Se entiende por *información* a todo mensaje (conjunto de datos) que al receptor le interese, le entienda o lo ignore antes de recibirlo. Por lo que, el término de *seguridad de la información* se refiere a la prevención y a la protección, a través de ciertos mecanismos, para evitar que ocurra de manera accidental o intencional la transferencia, modificación, fusión o destrucción no autorizada de la información.

Por lo que *informática* es la información automatizada que es accedida a través de la tecnología asociada a la información, es decir, a través de medios automatizados.

Por lo tanto, podemos definir a la Seguridad Informática como:

"*El conjunto de normas, mecanismos, herramientas, procedimientos y recursos orientados a brindar protección a la información resguardando sus disponibilidad, integridad y confidencialidad"* (López Barrientos & Quezada Reyes, 2006).

Por ello la seguridad abarca muchos temas aparentemente dispares, como el mantenimiento regular de equipos, la ocultación de datos, la protección de los mismos con claves de acceso o protocolos de administración de una red.

3.2.1 Importancia de la SI

Es necesaria la Seguridad de la Información por la existencia de personas ajenas a la información, también conocidas como piratas informáticos o hackers, que buscan tener acceso a una red para modificar, sustraer o borrar datos.

Tales personajes pueden, incluso, formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el área, más de 70 por ciento de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

3.2.2 Elementos a proteger

Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Son tres elementos que conforman los activos:

1. ***Información*:** Es el objeto de mayor valor para una organización, el objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.

2. ***Equipos que la soportan*:** Software, hardware y organización.

3. ***Usuarios:*** Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

3.3 Estándares de Seguridad Informática

Los estándares de seguridad son una herramienta que apoya la gestión de la seguridad informática, ya que los ambientes cada vez más complejos requieren de modelos que administren las tecnologías de manera integral, sin embargo, existen distintos modelos aplicables en la administración de la seguridad.

3.3.1 Trusted Computer Security Evaluation Criteria. TCSEC.

El Departamento de Defensa de los Estados Unidos por los años 80's (1983-1985) publica una serie de documentos denominados Serie Arco iris (**Rainbow Series**). Dentro de esta serie se encuentra el Libro Naranja (**Orange Book**) el cual suministra especificaciones de seguridad. Se definen siete conjuntos de criterios de evaluación denominados clases (D, C1, C2, B1, B2, B3 y A1). Cada clase de criterios cubre cuatro aspectos de la evaluación: política de seguridad, imputabilidad, aseguramiento y documentación. Los criterios correspondientes a estas cuatro áreas van ganando en detalle de una clase a otra, constituyendo una jerarquía en la que D es el nivel más bajo y A1 él más elevado. Todas las clases incluyen requisitos tanto de funcionalidad como de confianza.

- **Nivel D** (Protección mínima)

Sin seguridad, está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad.

- **Nivel C1** (Protección Discrecional)

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "súper usuario"; quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, debido a que no hay forma de distinguir entre los cambios que hizo cada usuario.

- **Nivel C2** (Protección de Acceso Controlado)

Este nivel fue diseñado para solucionar las debilidades del **C1**. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos.

Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoria es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios.

La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores.

- **Nivel B1** (Seguridad Etiquetada)

Soporta seguridad multinivel, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados.

También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

- **Nivel B2** (Protección Estructurada)

La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

- **Nivel B3** (Dominios de seguridad)

Este nivel requiere que la Terminal del usuario se conecte al sistema por medio de una conexión segura. Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y pruebas ante posibles violaciones.

- **Nivel A1** (Protección verificada)

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

Por la década de los 90's se publicó Minimum Security Functionality Requirements (MSFR) por el National Institute of Standards and Technology (NIST). En 1992 se creó Federal Criteria.

3.3.2 Information Technology Security Evaluation Criteria. ITSEC.

Por su parte el Information Technology Security Evaluation Criteria (ITSEC), conformado principalmente por Francia, Alemania y Reino Unido, crearon su propio estándar de seguridad, al principio de los 90's, este se conoce como el Libro Blanco (White Book)

Se definen siete niveles de evaluación, denominados E0 a E6, que representan una confianza para alcanzar la meta u objetivo de seguridad. E0 representa una confianza inadecuada. E1, el punto de entrada por debajo del cual no cabe la confianza útil, y E6 el nivel de confianza más elevado.

La correspondencia que se pretende entre los criterios ITSEC y las claves TCSEC es la siguiente:

Tabla 3.1. Correspondencia entre los criterios ITSEC y las claves TCSEC

Criterios ITSEC	Claves TCSEC
E0	D
F-C1, E1	C1
F-C2, E2	C2
F-B1, E3	B1
F-B2, E4	B2
F-B3, E5	B3
F-B3, E6	A1

Por su parte Canadá en 1993 publico Canadian Trusted Computer Product Evaluation Criteria (**CTCPEC**).

Estos documentos no satisfacían las exigencias de seguridad de los diversos países involucrados, por lo cual se creó un documento que unificará estos criterios dando origen a los Criterios Comunes.

3.3.3 ISO 15408 Criterios Comunes (CC).

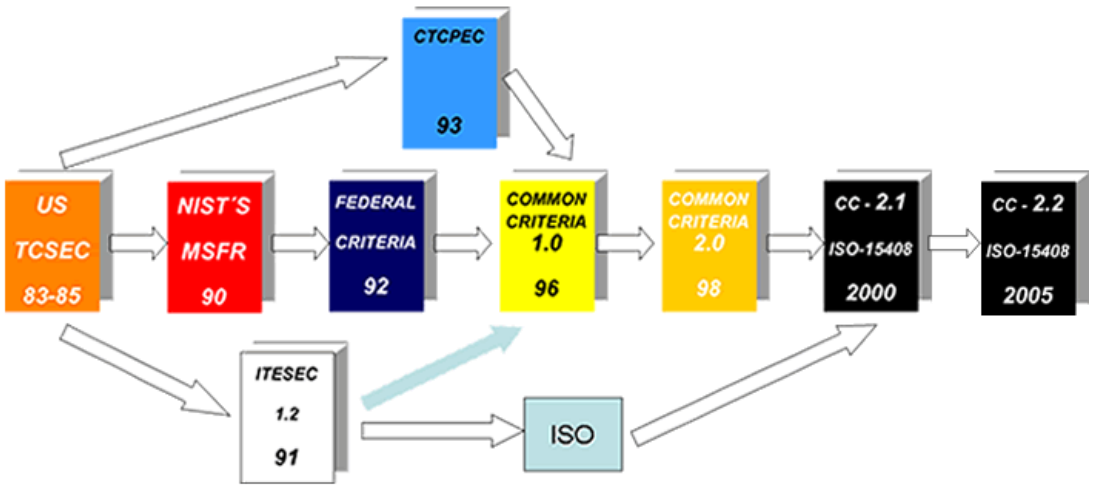


Figura 3.1. Generación de Criterios Comunes

Los CC (Criterios Comunes) su primer versión surgió en el 96, pero Europa paralelamente trabajó en un estándar ISO, esto nos regresaba al problema original, tener criterios diferentes de seguridad dependiendo del continente en el que se encontrará; para el año 2000 se unificaron criterios nuevamente dando lugar a un estándar internacional que puede ser conocido con el nombre de Common Criteria o ISO-15408.

En el año del 2005 se actualizaron los CC dando origen a CC versión 2.2 también conocido como ISO-15408:2005

Pero porque son tan importantes los CC en la Seguridad de la Información (SI). En principio es un estándar internacional aceptado por una gran cantidad de países como son:

- Canadá
- Francia
- Alemania

- Reino Unido
- Estados Unidos
- Australia
- Nueva Zelanda
- Finlandia
- Grecia
- Italia
- Holanda
- Noruega
- España

Los CC nos ofrecen una norma internacional para evaluar la seguridad de los productos de tecnología de la información. Se puede pensar en tres diferentes perspectivas desde las cuales los podemos abordar:

- Como consumidores proveen criterios que determinan las necesidades de seguridad que deben cumplir los productos que se deseen adquirir.
- Como desarrolladores proveen criterios que permite cubrir requerimientos de seguridad en diferentes niveles
- Como evaluadores proporcionan los productos de seguridad que deben ser cubiertos por los desarrolladores.

Los CC están divididos en 3 partes:

- Introducción y Modelo General.
- Requerimientos Funcionales.
- Requerimientos de Garantía.

A veces se tiene la idea de que no es bueno utilizar CC para implementar un esquema de seguridad, porque se piensa que no son certificables debido a que son muy generales. Por esta razón se usan estándares como pueden ser el ISO-17799 o el ISO-27000.

3.3.4 BS 7799 (Reino Unido)

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización inglesa equivalente a AENOR en España) 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 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.

El estándar británico BS 7799 es un estándar aceptado ampliamente que ha sido utilizado como base para elaborar otros estándares de seguridad de la información incluyendo el ISO 17799

La versión actual de estándar tiene dos partes:

- BS7799-1:1999 Information Security Management. Code of Practice for Information Security Management. Es la guía de buenas prácticas, para la que no se establece un modelo de certificación.
- BS7799-2:1999 Information Security Management. Specification for Information Security Management Systems, establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

3.3.5 ISO 17799

El estándar de seguridad de la información ISO 17799, es descendiente del BS 7799 – Information Security Management Standard – de la BSI (British Standard Institute) que publicó su primera versión en Inglaterra en 1995, con actualizaciones realizadas en 1998 y 1999, consiste de dos partes:

- *Parte 1:* Código de prácticas.
- Parte 2: Especificaciones del sistema de administración de seguridad de la información.

Por la necesidad generalizada de contar con un estándar de carácter internacional que permitiera reconocer o validar el marco de referencia de seguridad aplicado por las organizaciones, se elaboró el estándar ISO17799:2000, basado principalmente en la primera parte del BS 7799 conocida como Código de Prácticas (BS 7799 Part 1: Code of Practice).

El ISO 17799, al definirse como una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios de la seguridad informática:

- **Confidencialidad.** Asegurar que únicamente personal autorizado tenga acceso a la información.

- **Integridad.** Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.
- **Disponibilidad.** Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno, educativas e investigación; no obstante, dependiendo de la naturaleza y metas de las organizaciones, éstas mostrarán especial énfasis en algún dominio o área del estándar ISO 17799.

3.3.5.1 Los controles del ISO 17799

El éxito de la implementación del estándar de seguridad ISO 17799 requiere de una serie de procedimientos donde, inicialmente, el análisis de riesgos identificará los activos de la información y las amenazas a las cuales se encuentra expuesta.

El análisis de riesgos guiará en la correcta selección de los controles que apliquen a la organización; este proceso se conoce en la jerga del estándar como Statement of Applicability, que es la definición de los controles que aplican a la organización con objeto de proporcionar niveles prácticos de seguridad de la información y medir el cumplimiento de los mismos.

A continuación, se describirán cada una de las diez áreas de seguridad con el objeto de esclarecer los objetivos de estos controles.

1. ***Políticas de seguridad.*** El estándar define como obligatorias las políticas de seguridad documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.

2. ***Seguridad organizacional*****.** Establece el marco formal de seguridad que debe integrar una organización, tales como un foro de administración de la seguridad de la información, un contacto oficial de seguridad (Information System Security Officer – ISSO), revisiones externas a la infraestructura de seguridad y controles a los servicios de outsourcing, entre otros aspectos.

3. ***Clasificación y control de activos.*** El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

4. ***Seguridad del personal.*** Proporcionar controles a las acciones del personal que opera con los activos de información.

El objetivo de esta área del estándar es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.

5. ***Seguridad física y de entorno.*** Identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

6. ***Comunicaciones y administración de operaciones.*** Integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.

7. ***Control de acceso.*** Habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

8. ***Desarrollo de sistemas y mantenimiento.*** La organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.

9. ***Continuidad de las operaciones de la organización.*** El sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.

10. ***Requerimientos legales.*** La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

Cada una de las áreas establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle.

3.3.6 ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

El ISO-27000 se basa en la segunda parte del estándar británico BS7799 (BS7799:2). Está compuesta a grandes rasgos por:

- ISMS(Information Security Management System).
- Valoración de Riesgo.
- Controles.

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

- **ISO 27000:** En fase de desarrollo. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma será gratuita, a diferencia de las demás de la serie, que tendrán un coste.

- **ISO 27001:** Es la norma principal de 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. Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última.

- En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), 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.

- **ISO 27002:** Cambio de nomenclatura de ISO 17799:2005 realizada el 1 de Julio de 2007. 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.

- **ISO 27003:** En fase de desarrollo; probable publicación a finales de 2008. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- **ISO 27004:** En fase de desarrollo; probable publicación a lo largo de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.

- **ISO 27005:** En fase de desarrollo; probable publicación a finales de 2007 ó principios de 2008. Consistirá en una guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI. Se basará en la BS7799-3 (publicada en Marzo de 2006) e ISO 13335-3.

- **ISO 27006:** Publicada en Febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

3.4 Servicios de Seguridad Informática

Un servicio de seguridad es aquel que mejora la seguridad de un sistema de información y el flujo de información de una organización. Los servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio.

Clasificación

Una clasificación muy utilizada de los servicios de seguridad es la siguiente:

- Confidencialidad
- Autenticación
- Integridad
- No repudio
- Control de acceso
- Disponibilidad

3.4.1 Confidencialidad

Servicio de seguridad o condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. También puede verse como la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

La confidencialidad es importante porque la consecuencia del descubrimiento no autorizado puede ser desastrosa. Los servicios de confidencialidad proveen protección de los recursos y de la información en términos del almacenamiento y de la información, para asegurarse que nadie pueda leer, copiar, descubrir o modificar la información sin autorización. Así como interceptar las comunicaciones o los mensajes entre entidades.

Mecanismos para salvaguardar la confidencialidad de los datos:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

3.4.2 Autenticación

Es el servicio que trata de asegurar que una comunicación sea auténtica, es decir, verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos también sean correctos.

Algunos métodos de autenticación son:

- Biomédicas, por huellas dactilares, retina del ojo, etc.
- Tarjetas inteligentes que guardan información de los certificados de un usuario
- Métodos clásicos basados en contraseña:
    - Comprobación local o método tradicional en la propia máquina
    - Comprobación en red o método distribuido, más utilizado actualmente

3.4.3 Integridad

Servicio de seguridad que garantiza que la información sea modificada, incluyendo su creación y borrado, sólo por el personal autorizado.

El sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. El problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales.

3.4.4 No repudio

El no repudio sirve a los emisores o a los receptores para negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

El no repudio se aplica al problema de denegación falsa de la información que se recibe de otros o de la que uno ha enviado a otros. Los servicios de no repudio suministran pruebas que pueden ser demostradas a una tercera entidad. Los siguientes servicios son los que pueden ser proporcionados:

- ***No repudio de origen:*** provee pruebas del origen de los datos, por lo tanto protege al receptor de que el emisor niegue haber enviado el mensaje.

- ***No repudio de envío:*** provee pruebas del envío de los datos, por lo tanto previene a quien recibe los datos de cualquier denegación falsa al recibir los datos.

- ***No repudio de presentación:*** provee pruebas de presentación de los datos, con ello protege contra cualquier intento falso de negar que los datos fueron presentados para el envío.

- ***No repudio de transporte:*** provee pruebas del transporte de los datos, con lo que protege contra cualquier intento de negar que los datos fueron transportados.

- ***No repudio de recepción:*** provee pruebas de recepción de los datos, con esto se protege al emisor de que el receptor niegue haber recibido el mensaje.

3.4.5 Control de acceso

Un control de acceso se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que entonces le sea permitido el acceso.

Los componentes básicos de un mecanismo de control de acceso son las entidades de red, los recursos de la red y los derechos de acceso. Estos últimos describen los privilegios de la entidad o los permisos con base en qué condiciones las entidades pueden tener acceso a un recurso de la red y cómo estas entidades son permitidas para tener acceso a un recurso de la red.

El control de acceso puede ejecutarse de acuerdo con los niveles de seguridad y puede ejecutarse mediante la administración de la red o por una entidad individual de acuerdo con las políticas de control de acceso.

3.4.6 Disponibilidad

En un entorno donde las comunicaciones juegan un papel importante es necesario asegurar que la red esté siempre disponible.

La disponibilidad es un servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información asociados en el lugar, momento y forma en que es requerido. Un sistema seguro debe mantener la información disponible para los usuarios. El sistema, tanto hardware como software, debe mantenerse funcionando eficientemente y ser capaz de recuperarse rápidamente en caso de fallo.

3.5 Amenazas

Una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño en los sistemas de información, produciendo pérdidas materiales, financieras o de otro tipo. Las amenazas

son múltiples desde una inundación, un fallo eléctrico o una organización criminal o terrorista. Así, una amenaza es todo aquello que intenta o pretende destruir.

Las amenazas se pueden clasificar en cinco tipos:

3.5.1 Humanas

Surge por ignorancia en el manejo de la información, por descuido, por negligencia, por inconformidad. Para este caso se pueden considerar a los *hackers, crakers, phreakers, carding, trashing, gurús, lamers o scriptkiddies, copyhackers, bucaneros, newbie, wannabers, samurai, creadores de virus y los que se listan a continuación:*

- ***Ingeniería social:*** es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan de forma que revelen datos indispensables que permitan superar las barreras de seguridad. Esta técnica es una de las más usadas y efectivas al momento de averiguar nombres de usuarios y contraseñas.

- ***Ingeniería social inversa:*** Consiste en la generación, por parte de los intrusos, de una situación inversa a la original en la ingeniería social. En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios y éstos lo llaman ante algún imprevisto. El intruso aprovechará esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el propio.

- ***Robo:*** Las computadoras son las posesiones más valiosas de la empresa y se encuentran expuestas. Es frecuente que los operadores utilicen las computadoras de las empresas para realizar trabajos privados o para otras organizaciones y de esta manera robar tiempo de máquina.

- ***Fraude:*** Cada año millones de dólares son sustraídos de las empresas y, en muchas ocasiones, las computadoras son utilizadas para dichos fines. Es uno de los problemas más habituales de las Organizaciones, sea del tipo que sea y a todos los niveles, ya que se refiere al perjuicio económico patrimonial realizado con ánimo de lucro y llevado a cabo con engaño. (Labodía Bonastre, 1994)

  El fraude no trata más que lograr un beneficio ilegal reduciendo las propiedades de la compañía.

- ***Sabotaje****:* El sabotaje ha sido utilizado desde la antigüedad, partiendo del axioma de "*una eficiencia máxima, con unos medios y un riesgo mínimo para el saboteador*" (Labodía Bonastre, 1994)

Para lograr estos fines el saboteador tratará de determinar los puntos débiles de la Organización y estudiará las posibilidades de acceder a las áreas donde mayor daño pueda hacer.

Es el peligro más temido en los centros de procesamiento de datos, ya que éste puede realizarlo un empleado o un sujeto ajeno a la empresa.

- ***Personal:*** De los robos, fraudes, sabotajes o accidentes relacionados con los sistemas, el 73% es causado por el personal de la organización propietaria de dichos sistemas.

- ***Personal interno:*** Son las amenazas al sistema provenientes del personal del propio sistema informático.

Los daños causados por el personal pueden ser accidentales, deliberados o productos de la negligencia. Los recursos y programas así como la información, deben estar especialmente protegidos contra estos tipos de daños (Rodriguez, 1995)

- ***Ex-empleado****:* Generalmente son personas descontentas con la organización y que conocen a la perfección la estructura del sistema, por consiguiente, tienen los conocimientos necesarios para causar cualquier tipo de daño.

- ***Curiosos:*** Son personas que tienen un alta interés en las nuevas tecnologías, pero aún no tienen la experiencia ni conocimientos básicos para considerarlos hacker o crackers, generalmente no se trata de ataques dañinos, pero afecta el entorno de fiabilidad y confiabilidad generado en un sistema.

- ***Terrorista:*** En esta definición se engloba a cualquier persona que ataca al sistema causando un daño de cualquier índole en él, tienen fines proselitistas o religiosos.

- ***Intrusos remunerados:*** Se trata de crackers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar secretos o simplemente para dañar de alguna manera la imagen de la entidad atacada.

3.5.2 Hardware

Este tipo de amenazas se da por fallas físicas que se encuentra presente en cualquier elemento de dispositivos que conforman la computadora. Los problemas más identificados para que el suministro de energía falle son el bajo voltaje, ruido electromagnético, distorsión, interferencias, alto voltaje, variación de frecuencia, etc.

3.5.3 Red

Se presenta una amenaza cuando no se calcula bien el flujo de información que va a circular por el canal de comunicación, es decir, que un atacante podría saturar el canal de comunicación provocando la no disponibilidad de la red. Otro factor es la desconexión del canal.

3.5.4 Lógicas

La amenaza se hace presente cuando un diseño bien elaborado de un mecanismo de seguridad se implementa mal, es decir, no cumple con las especificaciones del diseño. La comunicación entre procesos puede resultar una amenaza cuando un intruso utilice una aplicación que permita evitar y recibir información, ésta podría consistir en enviar contraseñas y recibir el mensaje de contraseña válida; dándole al intruso elementos para un posible ataque.

En la mayoría de los sistemas, los usuarios no pueden determinar si el hardware o el software con que funcionan son los que supone que deben ser. Esto facilita al intruso para que pueda reemplazar un programa sin conocimiento del usuario y éste pueda inadvertidamente teclear su contraseña en un programa de entrada falso al cual también se le denomina códigos maliciosos.

Los tipos de códigos maliciosos más comunes son: caballos de Troya, virus, gusanos, bombas de tiempo y keyloggers.

a) Caballos de Troya

Es un programa aparentemente útil que contiene funciones escondidas y además pueden explotar los privilegios de un usuario dando como resultado una amenaza hacia la seguridad. Un caballo de Troya es más peligroso que un administrador del sistema o un usuario con ciertos privilegios, ya que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final; esto es, que se presente como información pérdida o basura, sin ningún sentido. Pero al cabo de algún tiempo, y esperando la indicación del programa, despierta y comienzan a ejecutarse y a mostrar sus verdaderas intenciones. También pueden aparentar ser un programa de juegos o entretener al usuario mostrando pantallas de espectáculos y sonidos agradables, mientras realizan operaciones dañinas para el sistema. (Cortés Ferreyra, 1995)

b) Virus

Un virus informático es un programa informático malicioso que cuando una personan confiada lo ejecuta, lleva a cabo tareas que incluyen fundamentalmente reproducirse a sí mismos y en algunos casos desplegar una carga dañina. Las principales forma de propagación son:

a) Medios de difusión externos: cualquier dispositivo de almacenamiento que puede contener un archivo de ordenador, como DVD, o CD, y pueda conectarse o insertarse en un ordenador.

b) Conexión a la red: Una red es un grupo de ordenadores conectados entre sí para poder intercambiar datos. Internet, que es la fuente virus más común, hoy en día, es una gran red. Los virus pueden usar la conexión de ordenador a ordenador (Walker, 2006)

Los virus son la principal amenaza en la red. Estos programas de extensión relativamente pequeña son capaces de replicarse o copiarse a sí mismos. Las tres vías de propagación más ampliamente conocidas son: un archivo anexo o adjunto al correo electrónico, una transferencia FTP, TELNET y muchos más, descargar un archivo infectado desde una página web.

c) Gusanos

Son programas que se reproducen a sí mismos y no requieren de un anfitrión, pues se arrastran literalmente por todo el sistema sin necesidad de un programa que los transporte. Los gusanos se cargan en la memoria y se posicionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente, esto hace que queden borrados los programas o información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdida de datos. (Cortés Ferreyra, 1995)

Los gusanos son programas que se propagan ellos mismos; un gusano hace una copia de sí mismo y lo realiza cuando es ejecutado. Los gusanos frecuentemente se propagan de una computadora a otra a través de las conexiones de la red. Los gusanos con frecuencia roban, destruyen o modifican datos en una computadora.

Los gusanos tienen como única misión la de colapsar cualquier sistema, ya que son programas que se copian en archivos distintos en cadena hasta crear miles de réplicas de sí mismos.

d) Bombas de Tiempo

Son programas ocultos en la memoria del sistema o en los discos, dentro de archivos de programas ejecutables con extensión .COM o .EXE. Esperan una fecha o una hora para explotar. Algunos de estos virus no son destructivos y sólo exhiben mensajes en la pantalla al llegar el momento de la explosión. Llegado el momento, se activa cuando se ejecuta el programa que las contiene. (Cortés Ferreyra, 1995)

e) Keyloggers

Los Keyloggers son programas para el espionaje que plantean muchos problemas éticos y legales. La función del Keyloggers es registrar todas las pulsaciones del teclado en un archivo del sistema para luego proceder a su lectura, de esta manera todo lo que se haya escrito, como nombres de usuario o contraseñas queda registrado en un archivo.

3.5 Fenómenos naturales que provocan desastres

Los diferentes fenómenos naturales que provocan desastres representan uno de los riesgos más fuertes y debido a la existencia de éstos se convierte en una de las razones por la cuales deben desarrollarse planes de contingencia y aplicarse medidas en pro de la seguridad de la información.

De acuerdo a Rodríguez (1995) la clasificación de fenómenos naturales que causan desastres utilizados en las Bases para el Establecimiento del Sistema Nacional de Protección Civil:

a) Geológicos

Tienen sus orígenes en la actividad de las placas tectónicas y fallas continentales y regionales que cruzan y circundan a la República Mexicana.

Como son:

- Sismos
- Vulcanismo
- Colapso de suelos
- Hundimiento regional y agrietamiento
- Algunas consecuencias de los sismos y erupciones tales como maremotos (tsunami) y lahares.

b) Hidrometeorológicos

Son los fenómenos que derivan de acción violenta de los agentes atmosféricos, como los huracanes, las inundaciones fluviales y pluviales, etc.

Como son:

- Lluvias
- Tormentas de granizo
- Inundaciones
- Temperaturas extremas
- Sequias

- Tormentas eléctricas
- Vientos

c) Químicos

Se encuentran estrechamente ligados a la compleja vida en sociedad, al desarrollo industrial y tecnológico de las actividades humanas, y al uso de diversas formas de energía.

Como son:

- Contaminantes
- Envenenamientos
- Incendios
- Explosiones
- Radiaciones

d) Sanitarios

Se vinculan con el crecimiento de la población y la industria. Sus fuentes se ubican en las grandes concentraciones humanas y vehiculares.

Como son:

- Epidemia
- Plagas

e) Socio-Organizativos

Tiene su origen en las actividades de las concentraciones humanas, y en el mal funcionamiento de algún sistema de subsistencia que proporciona servicios básicos.

Como son:

- Explosión demográfica
- Fallas humanas
- Disturbios sociales
- Actos delictivos
- Accidentes
- Acciones bélicas
- Drogadicción-alcoholismo
- Efectos negativos producidos por la operación actual de servicios
- Interrupción de servicios

3.6 Vulnerabilidades

La vulnerabilidad de un sistema informático son todas aquellas debilidades que se están presentando en el sistema, lo cual hace susceptible de ser afectado, alterado o destruido por alguna circunstancia indeseada, que afectan al funcionamiento normal o previsto de dicho sistema informático.

De acuerdo a (López Barrientos & Quezada Reyes, 2006), las vulnerabilidades se pueden clasificarse en seis tipos:

3.6.1 Física

Lo podemos encontrar en el edificio o entorno físico. La relacionamos con la posibilidad de entrar o acceder físicamente al lugar donde se encuentra el sistema para robar, modificar o destruir el mismo. Esta vulnerabilidad se refiere al control de acceso físico al sistema.

Para un servidor se puede plantear mecanismos estrictos de seguridad en este punto, pero para una computadora personal donde pueden acceder al lugar más de una persona autorizada es difícil de llevar un control, para ese caso, se podrían implementar medidas vía software para impedir el robo de información, el acceso a periféricos, pero aun así quedan vulnerables los medios físicos que almacenan datos de forma externa a la computadora personal, como son CD-ROM, DVD, USB, discos duros externos, hojas impresas.

3.6.2 Natural

Se refiere al grado en que el sistema puede verse afectado debido a los fenómenos naturales que causan desastres.

Las vulnerabilidades pueden ser:

- No contar con un espejo del sistema en otro lugar geográfico en caso de inundaciones o terremotos.

- No disponer de reguladores, no-breaks, plantas de energía eléctrica alterna

- Tener una mala instalación eléctrica de los equipos, en caso de rayos, fallas eléctricas o picos altos de potencia.

- Además de que las instalaciones se encuentren en mal estado, no contar con un adecuado sistema de ventilación y calefacción para que los equipos en temperaturas de 18 y 21 °C y se tenga una humedad entre 48 y 65%

- En caso de inundaciones, el no contar con paredes, techos impermeables y puertas que no permitan el paso del agua.

- No estar informado de las condiciones climatológicas locales al construir un centro de cómputo o para tomar medidas en determinado tiempo.

Las vulnerabilidades que se pueden tener en caso de incendio son:

- El área donde se encuentran las computadoras está en un local combustible o inflamable.

- El centro de cómputo está situado encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.

- Las paredes no están hechas de material contra incendio y no están extendidas desde el suelo al techo.

- Que no se cuente con un piso falso instalado sobre el piso real con materiales no combustibles y resistentes al fuego.

- Que se pueda fumar en los centros de cómputo.

- El no contar con muebles no combustibles y cestos metálicos para papeles o se tengan materiales de plástico inflamables.

- El no contar con equipos para la extinción de incendios en relación con el grado de riesgo y la clase de fuego que sea posible en ese ámbito, además de no contar con extintores manuales (portátiles) y automáticos (rociadores).

- El no tener los medios para proteger al sistema de daños causados por el humo

- El no contar con procedimientos planeados para recibir y almacenar abastecimientos de papel, ya que este material es por lo general el que empeora el fuego.

3.6.3 De hardware

El no verificar las características técnicas de los dispositivos junto con sus respectivas especificaciones, la falta de mantenimiento del equipo. Desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros. Así, pueden existir algunos sistemas que no cuenten con la herramienta o tarjeta para poder acceder a los mismos; adquirir un equipo de mala calidad o hacer un mal uso del mismo, tener el equipo de cómputo expuesto a cargas estáticas, etc.

3.6.4 De software

Ciertas fallas o debilidades de los programas del sistema hace más fácil acceder al mismo y lo hace menos confiable. Este tipo de vulnerabilidades incluye todos los errores de programación en el sistema operativo u otros de aplicaciones que permite atacar al sistema operativo desde la red explotando la vulnerabilidad en el sistema.

3.6.5 De red

La conexión de las computadoras a las redes supone un enorme incremento de la vulnerabilidad del sistema, aumenta considerablemente la escala de riesgos a que está sometido, al aumentar la cantidad de gente que puede tener acceso al mismo o intenta tenerlo. También se añade el riesgo de intercepción de las comunicaciones:

- Se puede penetrar al sistema a través de la red.
- Interceptar información que es transmitida desde o hacia el sistema.

Se debe tener cuidado en que el centro de cómputo no tenga fallas debido a una mala estructura y en el diseño del cableado estructurado por no seguir ningún estándar para el diseño e implementación del mismo.

3.6.6 Humana

Algunas de las diferentes vulnerabilidades humanas se tienen:

- Contratar personal sin perfil psicológico y ético
- No tener personal suficiente para todas las tareas
- El descuido
- El cansancio
- Maltrato del personal, así como la mala comunicación con el personal, malos entendidos
- Personal irresponsable, que descuida el acceso a su área de trabajo
- No tener servicio técnico propio de confianza
- No instruir a los usuarios para que eviten responder a preguntas sobre cualquier característica del sistema
- No asegurarse de que las personas que llaman por teléfono son quienes dicen ser
- El no tener control de acceso o acceso basado en restricciones de tiempo

- No contar con guardias de seguridad

- No tener un control de registros de entrada y salida de las personas que visitan el centro de cómputo

- No contar con credenciales de identificación del personal y no contar con algún detector biométrico, como: emisión de calor, huella digital, verificación de voz o verificación de huellas oculares.

- No disponer de algún sistema de protección eléctrica como: barreras infrarrojas o de microondas, detector de ultrasonido, detectores pasivos sin alimentación, sincronización o dispositivos luminosos, edificios inteligentes, etc.

3.7 Ataques

Un ataque es un evento exitoso o no, que atenta sobre el buen funcionamiento del sistema.

En el flujo normal de la información (figura 3.2) no debe existir ningún tipo de obstáculos para que la información llegue al destinatario.

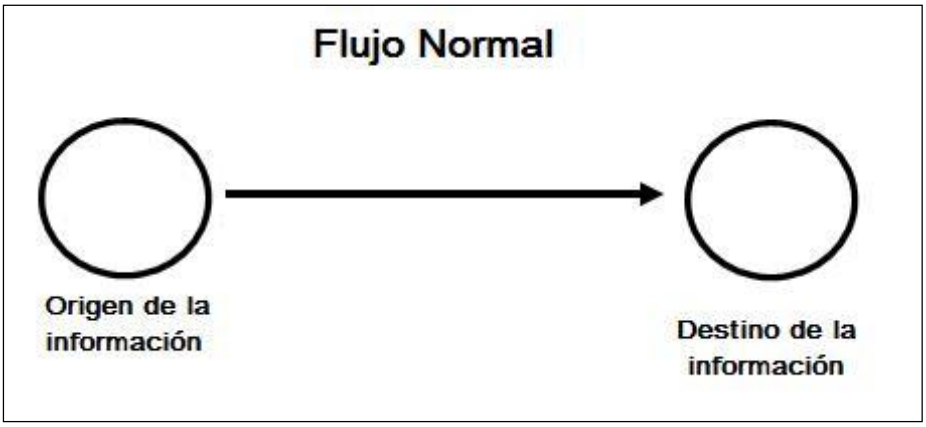


Figura 3.2 Flujo Normal de la información

Las cuatro categorías generales de amenazas o ataques son las siguientes:

3.7.1 Interrupción

Un recurso del sistema es destruido o se vuelve no disponible (figura 3.3). Este es un ataque contra la *disponibilidad.* Ejemplos de estos ataques: destrucción de un elemento de hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

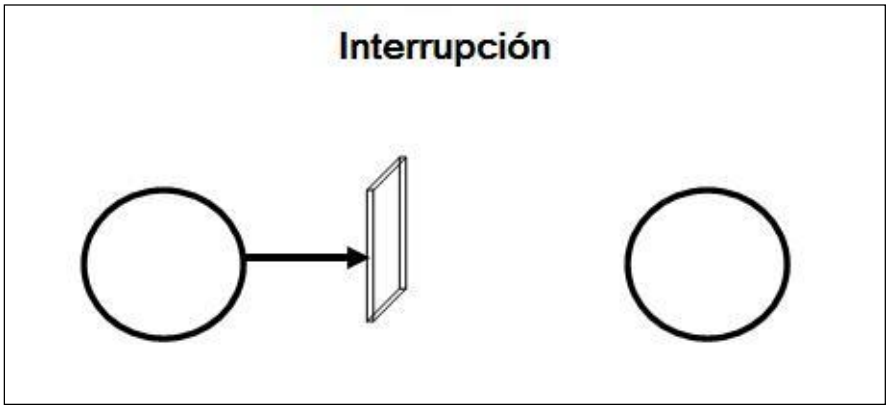


Figura 3.3 Flujo con interrupción

3.7.2 Intercepción

Intercepción se produce cuando un programa, proceso o persona accede a una parte del sistema para la cual no tiene autorización (figura 3.4). Es el incidente de seguridad más difícil de detectar, ya que generalmente no produce una alteración en el sistema. Este es un ataque en contra de la *confidencialidad.* Ejemplos de este tipo de ataque: acceso a una base de datos, entrada a través de la red en un sistema informático ajeno, etc.

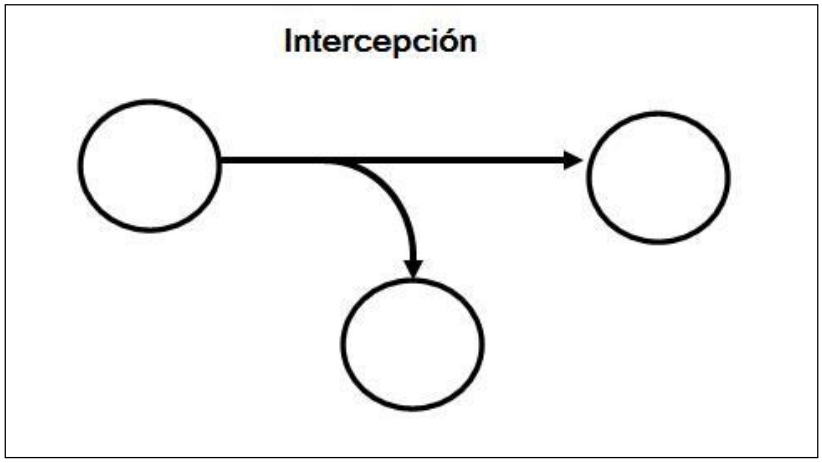


Figura 3.4 Flujo con intercepción

3.7.3 Modificación

Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo (figura 3.5). Es el tipo de amenaza más peligroso ya que puede ocasionar grandes daños en el sistema. Este es un ataque contra la *integridad*. Ejemplos de este tipo de ataque: cambios en el contenido de una base de datos, cambios en los datos de una transferencia bancaria, etc.

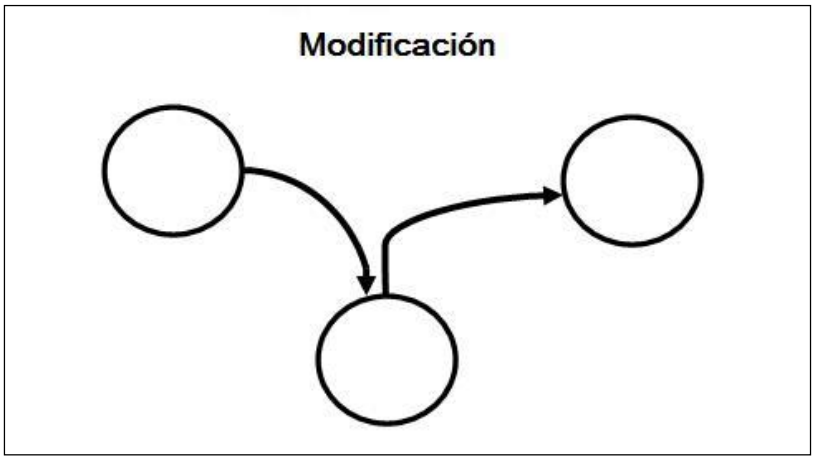


Figura 3.5 Flujo con modificación

3.7.4 Suplantación o fabricación

Una entidad no autorizada inserta objetos falsificados en el sistema (figura 3.6). Este es un ataque contra la *autenticidad*. Ejemplos de este tipo de ataques: virus informáticos, caballos de Troya, transacciones electrónicas falsas, introducción de datos en una base, etc.

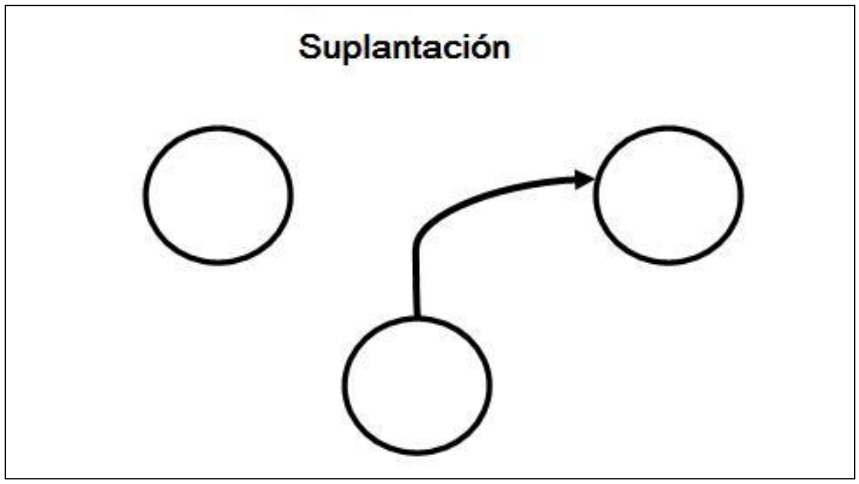


Figura 3.6 Flujo con suplantación

3.7.5 Métodos de Ataque

Un ataque en un sistema de cómputo contempla tres etapas principales:

1. *Preparación:* el método de ataque se plantea u otras preparaciones se realizan.

2. *Activación:* el ataque se activa o dispara

3. *Ejecución:* la misión se lleva a cabo mediante la desviación de los controles de acceso, violación de secretos o integridad, denegación de servicio, robo de servicios, o simplemente dar a conocer el ataque.

Preparación y planteamiento

Algunas formas de efectuar esta primera etapa son:

- *Recolección de la información:* los individuos que poseen ciertos derechos sobre la información o flujos de información secreta, simplemente recolectan la del sistema que están autorizados a monitorear, sin embargo, las personas externas deben ingeniárselas para obtenerlas, esto pude lograrse a través de engaños, basándose principalmente en convencer a la gente de haga lo que en realidad no debería.

- *Caballo de Troya:* un usuario coloca un programa dentro de su dominio de protección, cuando el programa se ejecuta, obtiene los privilegios de dicho usuario, de esta manera se convierte en un cómplice inconsciente ya que envía y concede información a los perpetradores de sus archivos (de forma no aparente).

- *Propagación programada:* se refiere al código malicioso que se introduce en un equipo de cómputo ya que puede multiplicar su ámbito y daño.

- *Puerta trasera:* el software contiene mecanismos ocultos que permiten a los diseñadores (o quienes sepan el secreto) desviar los controles.

- *Enmascaramiento o engaño:* significa que se pretende ser alguien más, de tal manera que se puede obtener los derechos de acceso de una persona. El enmascaramiento envuelve un ataque en los controles de autenticación, por lo que el sistema puede enmascararse como otro sistema para engañar al usuario y descubrir información.

- *Exploración:* consiste en el enviar una secuencia de información cambiante a una computadora para encontrar valores que muestren respuestas positivas, como son las contraseñas, números telefónicos, etc.

- *Mal uso de la autoridad:* si el atacante penetra de manera legítima al sistema, la preparación es mucho más fácil ya que está haciendo mal uso de la autoridad que posee dentro de la organización.

Activación

La activación puede realizarse de las siguientes maneras:

- Si el ámbito de preparación asume el control de una interrupción de un sistema operativo, el código de ataque es invocado cuando la interrupción se lleva a cabo, si no es así, el perpetrador puede invocar directamente un programa que lleve a cabo la misión.

- Un ataque más sofisticado impone un retardo entre la preparación y la activación, el retardo puede provocar que el ataque sea más destructivo, hablando específicamente de los virus.

- Una bomba de tiempo se encuentra arreglada para estallar a una hora y día determinados.

Ejecución

La ejecución del ataque está sustentada en la misión que se tenga y en esta tercera etapa las misiones pueden ser:

a) Mal uso activo

Afecta la integridad de la información o disponibilidad de los servicios. Los archivos pueden ser destruidos o sutilmente alterados.

b) Mal uso pasivo

Cuando la confidencialidad es violada pero el estado del sistema no es afectado, el mal uso es pasivo pero no por eso menos dañino, de hecho, podría resultar más letal que el activo. Algunas técnicas empleadas son:

- *Fisgoneo (la intromisión no autorizada):* abarca desde el escuchar de manera sofisticada lo que se transmite en una ruta de comunicación, hasta mirar por arriba de los hombros de un usuario lo que éste escribiendo con el teclado.

- *Residuo:* algunas amenazas explotan la no protección a los objetos que guardan la información como son los discos, segmentos de memoria, ya que el objeto es reutilizado por otro usuario sin que se le borre la información.

- *Hojeo:* se refiere a la búsqueda ociosa a través del almacenaje (información disponible) sin saber exactamente qué información se busca o si existe.

- *Interferencia:* junta piezas de información accesible para llegar a la información que se supone es secreta.

- *Canales encubiertos:* es la forma en que las personas puedan transferirse información de manera sutil (que se supone es secreta) utilizando canales que no son dedicados para esos propósitos.

- *Denegación de servicios:* cualquier tipo de caída traumática, interrupción de la energía o falla de una PC infectada por virus, deniega el servicio.

- *Robo de servicios:* el robo de servicios en un sistema hace que el servicio (proceso, flujo de información, etc.) se vuelva tan lento que llegue a la denegación de servicio.

CAPÍTULO 4

Esquemas de Seguridad Informática

En este capítulo se presentan diferentes esquemas de Seguridad Informática como son las Políticas de Seguridad, los procedimientos y planes de contingencia, los perfiles de protección y análisis de riesgos, donde se muestra la definición de cada una de ellas, así como los elementos que las integran y los diferentes métodos, modelos o pasos que se encuentran dentro de ellas.

CAPÍTULO 4

Esquemas de Seguridad Informática

4.1 Políticas de Seguridad

Las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

4.1.1 Definición de Política

La política de seguridad es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma. (López Barrientos & Quezada Reyes, 2006).

Las políticas de seguridad definen lo que está permitido y lo que está prohibido, permiten definir los procedimientos y herramientas necesarias, expresan el consenso de los "dueños" y permiten adoptar una buena actitud dentro de la organización (Daltabuit Godás, Hernández Audelo, Mallén Fullerton, & Vázquez Gómez, 2007).

4.1.2 Criterios de las OCDE[1]

La OCDE considera que los elementos de las políticas son:

1) Concienciación

Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.

El conocimiento de los riesgos y de los mecanismos disponibles de salvaguardia, es el primer paso en la defensa de la seguridad de los sistemas y redes de información. Estos sistemas y redes de información pueden verse afectados tanto por riesgos internos como externos. Los participantes deben comprender que los fallos en la seguridad pueden

[1] Véase "Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad", Organisation for Economic Co-operation and Development (OECD), París. y Ministerio de Administraciones Públicas, Secretaría General Técnica, España.

dañar significativamente los sistemas y redes que están bajo su control. Deben asimismo ser conscientes del daño potencial que esto puede provocar a otros derivados de la interconexión y la interdependencia. Los participantes deben tener conocimiento de las configuraciones y actualizaciones disponibles para sus sistemas, así como su lugar que ocupan dentro de las redes, las prácticas a ejecutar para ampliar la seguridad, y las necesidades del resto de los participantes.

2) Responsabilidad

Todos los participantes son responsables de la seguridad de los sistemas y redes de información.

Los participantes dependen de los sistemas y redes de información local y global, y deben comprender su responsabilidad en la salvaguarda de la seguridad de los sistemas y redes de información. Asimismo deben responder ante esta responsabilidad de una manera apropiada a su papel individual. Los participantes deben igualmente revisar sus propias políticas, prácticas, medidas y procedimientos de manera regular, y evaluar si éstos son apropiados en relación con su propio entorno. Aquellos que desarrollan y diseñan o suministran productos o servicios deberán elevar la seguridad de los sistemas y redes, y distribuir a los usuarios de manera apropiada información adecuada en materia de seguridad, incluyendo actualizaciones, para que éstos entiendan mejor la funcionalidad de la seguridad de sus productos y servicios, así como la responsabilidad que les corresponde en materia de seguridad.

3) Respuesta

Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.

Al reconocer la interconexión de los sistemas y de las redes de información, así como el riesgo potencial de un daño que se extienda con rapidez y tenga un alcance amplio, los participantes deben actuar de manera adecuada y conjunta para enfrentarse a los incidentes que afecten la seguridad. Asimismo han de compartir información sobre los riesgos y vulnerabilidades y ejecutar procedimientos para una cooperación rápida y efectiva que permita prevenir, detectar y responder a incidentes que afecten a la seguridad. Cuando sea posible, estas actuaciones habrán de suponer un intercambio de información y una cooperación transfronteriza.

4) Ética

Los participantes deben respetar los intereses legítimos de terceros.

Debido a la permeabilidad de los sistemas y de las redes de información en nuestras sociedades, los participantes necesitan reconocer que sus acciones o la falta de éstas, pueden comportar daños a terceros. Es crucial mantener una conducta ética, debiendo los participantes hacer esfuerzos por desarrollar y adoptar buenas prácticas y promover conductas que reconozcan la necesidad de salvaguardar la seguridad y respetar los intereses legítimos de terceros.

5) Democracia.

La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.

La seguridad debe lograrse de manera consistente con garantía de los valores reconocidos por las sociedades democráticas, incluyendo la libertad de intercambio de pensamiento e ideas, así como el libre flujo de información, la confidencialidad de la información y la comunicación y la protección apropiada de información personal, apertura y transparencia.

6) Evaluación del riesgo

Los participantes deben llevar a cabo evaluaciones de riesgo.

La evaluación del riesgo identificará las amenazas y vulnerabilidades, y debe ser lo suficientemente amplia para incluir factores internos y externos fundamentales como tecnología, factores físicos y humanos, y políticas y servicios de terceros que tengan repercusiones en la seguridad. La evaluación del riesgo permitirá determinar los niveles aceptables de seguridad y ayudar en la selección de controles apropiados para administrar el riesgo de daños potenciales a los sistemas y redes de información, en relación a la naturaleza e importancia de la información que debe ser protegida. Debido a la creciente interconexión de los sistemas de información, la evaluación del riesgo debe incluir asimismo consideraciones acerca del daño potencial que se puede causarse a terceros o que pueden tener su origen en terceras personas.

7) Diseño y realización de la seguridad.

Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.

Los sistemas, las redes y las políticas deberán ser diseñados, ejecutados y coordinados de manera apropiada para optimizar la seguridad. Un enfoque mayor pero no exclusivo de este esfuerzo ha de encontrarse en el diseño y adopción de mecanismos y soluciones que salvaguarden o limiten el daño potencial de amenazas o vulnerabilidades identificadas. Tanto las salvaguardas técnicas como las no técnicas así como las soluciones a adoptar se hacen imprescindibles, debiendo ser proporcionales al valor de la información de los sistemas y redes de información. La seguridad ha de ser un elemento fundamental de todos los productos, servicios, sistemas y redes; y una parte integral del diseño y arquitectura de los sistemas. Para los usuarios finales el diseño e implementación de la seguridad radica fundamentalmente en la selección y configuración de los productos y servicios de sus sistemas.

8) Gestión de la Seguridad.

Los participantes deben adoptar una visión integral de la administración de la seguridad.

La gestión de la seguridad debe estar basada en la evaluación del riesgo y ser dinámica, debiendo comprender todos los niveles de las actividades de los participantes y todos

los aspectos de sus operaciones. Asimismo ha de incluir posibles respuestas anticipadas a riesgos emergentes y considerar la prevención, detección y respuesta a incidentes que afecten a la seguridad, recuperación de sistemas, mantenimiento permanente, revisión y auditoría. Las políticas de seguridad de los sistemas y redes de información, así como las prácticas, medidas y procedimientos deben estar coordinadas e integradas para crear un sistema coherente de seguridad. Las exigencias en materia de gestión de seguridad dependerán de los niveles de participación, del papel que desempeñan los participantes, del riesgo de que se trate y de los requerimientos del sistema.

9) Reevaluación

Los participantes deben revisar y reevaluar la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

De manera constante se descubren nuevas amenazas y vulnerabilidades. Los participantes deberán, en este sentido, revisar y evaluar, y modificar todos los aspectos de la seguridad de manera continuada, a fin de poder enfrentarse a riesgos siempre en evolución permanente.

4.1.3 Postura

De acuerdo a (Daltabuit Godás, Hernández Audelo, Mallén Fullerton, & Vázquez Gómez, 2007), la confianza es el principio básico que rige el desarrollo de políticas. Lo primero es determinar quién tiene privilegios, y hay que *usar el principio del mínimo privilegio posible.*

Hay que tener cuidado en que tanto se confía en el personal. Se otorgan privilegios a medida que se necesitan y se requieren controles técnicos para asegurar que no se den violaciones.

Adoptar el modelo "Todo lo que no esté específicamente prohibido está permitido" o bien "Todo está prohibido excepto lo que esté específicamente permitido".

4.1.4 Beneficios

Las políticas de seguridad informática muchas veces ayudan a tomar decisiones sobre otros tipos de política (propiedad intelectual, destrucción de la información, etc.). También son útiles al tomas decisiones sobre adquisiciones porque algunos equipos o programas no serán aceptables en términos de las políticas mientras que otras la sustentaran.

Las políticas de seguridad informática deben considerarse como un documento de largo plazo, que evolucionan. No contienen asuntos específicos de implementación, pero si

asuntos específicos del equipo de cómputo y telecomunicaciones de la organización. Probablemente serán la guía para el diseño de cambios a esos sistemas.

El desarrollo e implantación de políticas de seguridad informática es una indicación de que una organización está bien administrada y los auditores lo toman en cuenta en sus evaluaciones. Condicen a una profesionalización de la organización (MacMillan R.).

4.1.5 Proceso del Diseño de Políticas

De acuerdo a (Daltabuit Godás, Hernández Audelo, Mallén Fullerton, & Vázquez Gómez, 2007), hay que especificar el alcance de las políticas y los objetos de las mismas, consistentemente con la misión de seguridad previamente establecida.

Las políticas promulgadas deben escribirse en párrafos que sean, cada uno por separado, implementarles mediante un mecanismo específico. Es decir, hay que procurar pensar claramente en la conveniencia de que las políticas sean sumamente específicas, si esto se puede lograr, es deseable fragmentar las políticas por departamento o unidad de trabajo. Pueden entonces pensarse en una jerarquía de políticas, unas con aplicabilidad general, y otras para aplicabilidad para grupos o tareas específicas.

Las políticas que no cuenten con la aceptación entusiasta de los usuarios de todos los niveles serán muy difíciles de implantar. Todos aquellos que serían afectados por las políticas deben tener la oportunidad de revisarlas y hacer comentarios antes de que se promulguen, deben contar con el apoyo total de los administradores.

En esta etapa deben considerarse los mecanismos de difusión, capacitación y concientización iniciales y permanentes sobre seguridad informática.

La cultura de la organización y sus necesidades de seguridad son un factor determinante para el equipo de redacción de las políticas. El nivel del control que se establezca no debe resultar en una reducción de la productividad, pues en muchos casos los ingresos y la carrera de la persona esta designadas por su productividad. Si son demasiadas restrictivas en comparación de la cultura organizacional se violarán las políticas.

Las razones que llevan la implantación de una política deben de explicarse dentro de la política misma. También debe definirse la cultura de cada política: quién, qué y cuándo.

4.1.6 Algunas políticas necesarias

De acuerdo a (Daltabuit Godás, Hernández Audelo, Mallén Fullerton, & Vázquez Gómez, 2007), hay que considerar las siguientes políticas necesarias:

a) Políticas de uso aceptable

Determina que se puede hacer con los recursos de cómputo (equipo y datos) de la organización. También determinan lo que no se puede hacer con esos recursos. Indica l responsabilidad de los usuarios en la protección de la información que manejan y en qué condiciones puede afectar o leer datos que no les pertenezca.

b) Políticas de cuentas de usuario

Determina el procedimiento que hay que seguir para adquirir privilegios de usuarios en uno o más sistemas de información y la vigencia de estos derechos.

Además quien tiene la autoridad de asignar estos privilegios y quienes no podrían recibir esos privilegios por causas legales. Debe exhibir explícitamente los deberes y derechos de los usuarios. Se explicara cómo y cuándo se deshabilitaran las cuentas de usuarios y que se hará con la información que contenga. Debe especificar claramente los detalles de los procedimientos de identificación y autenticación.

c) Políticas de acceso remoto

Se definen y explican los métodos aceptables para conectarse a los sistemas de información de la organización desde el exterior de la misma. Son particularmente para organizaciones geográficamente extendidas o aquellas cuyos miembros pasa la mayor parte del tiempo viajando. Además de establecer quien tiene derecho a este tipo de conexión también establecen quienes pueden emplear módems para conectarse al exterior de la organización, sobre todo módems de alta velocidad.

d) Políticas de la protección de la información

El objetivo es evitar que la información sea modificada o difundida durante su proceso, almacenamiento o transmisión. Específica como deben establecerse jerarquías de confidencialidad e integridad, y como se implementan su protección. Debe ponerse especial atención a la divulgación y la destrucción de la información.

e) Políticas de configuración del cortafuego

Establece quien determina el establecimiento y los cambios de la configuración. También quién debe tener acceso a ser usuario del cortafuego y quién puede obtener información acerca de la configuración del mismo. Debe establecer los de administración de la configuración, para que responda a las necesidades de la organización.

f) Políticas de cuentas privilegiadas

Establece los requisitos que debe satisfacer quienes usen cuentas privilegiadas (root, bkup, admin) en cuanto a su biografía y trayectoria dentro de la organización. Contienen procedimientos de la auditoria del uso de este tipo de cuentas, particularmente sobre los procedimientos de identificación y autenticación, y su uso. Determina en qué condiciones se debe cancelar el acceso privilegiado.

g) Políticas de conexión a la red

Define los requisitos que deben cumplirse para que se conecten nuevos dispositivos a la red de la organización. Son particularmente importantes para organizaciones que tienen una diversidad de equipos de soporte técnico, y para aquellos que no están protegidos con un cortafuegos. Deben especificar quien puede instalar nuevos recursos en la red, cuál es la autorización requerida y como se documentan los cabios. Deben aclarar cómo se manejan los dispositivos inseguros.

4.1.7 Restricciones a las políticas

La principal fuente de restricciones es la pérdida de productividad. Es inevitable que la implementación políticas de seguridad informática distraiga recursos humanos e informáticos que se podían emplear para otros fines.

Otra fuente de restricciones son la legislación y los derechos de los empleados y de los clientes. Cada país tiene su propia cultura, así como cada organización tiene la propia. Las políticas deben ajustarse al entorno cultural en el que estén inmersas y ciertamente no pueden violar la legislación vigente localmente.

4.1.8 Procedimientos

Una vez que se han determinado las políticas de seguridad que especifican lo que hay que proteger, es necesario realizar los procedimientos de seguridad que indican como hay que llevar a cabo la protección. Estos procedimientos también constituyen los mecanismos para hacer las políticas. Además resultan útiles, pues indican detalladamente que hay que hacer cuando sucedan incidentes específicos, son referencias rápidas en casos de emergencia y ayudan a eliminar los puntos de falla críticos.

A continuación se menciona algunos procedimientos que son necesarios, de acuerdo a (Daltabuit Godás, Hernández Audelo, Mallén Fullerton, & Vázquez Gómez, 2007):

a) Auditoría de la seguridad de los sistemas

Dado que los datos que se almacenan sobre el uso de los sistemas son la principal herramienta para detectar violaciones a las políticas, es necesario especificar detalladamente lo que se desea almacenar.

Como se resguardan estas bitácoras y quien tiene acceso a ellas.

b) Administración de cuentas

Abarca desde cómo se tiene que solicitar una cuenta en su sistema de información, o en varios sistemas hasta qué tienen que hacer el departamento de personal antes de despedir a un empleado. También lo que debe hacerse para cambiar los privilegios de una cuenta o cancelarla. Especifican como se documentan el manejo de las cuentas y como se vigila el cumplimiento de las políticas correspondientes.

c) Administración de autenticadores

Hay cuatro tipos de autenticadores: mediante conocimientos, características físicas, objetos y ubicación geográfica. Los sistemas de control de acceso, en general deben emplear por los menos dos autenticadores de tipos de distintos para cada usuario. Estos procedimientos indican como deben obtenerse los autenticadores, como deben resguardarse, la vigencia de los mismos y las características que deben tener. Por ejemplo el procedimiento de uso de contraseñas indicará su longitud, su posición, el algoritmo de cifrado que se debe emplear para archivarlas y resguardarlas. En el caso de autenticadores biométricos se especifican la característica seleccionada, los algoritmos que permiten uso, cómo se puede evitar que se construya la característica y como se debe archivar y resguarda los datos correspondientes.

d) Administración de la configuración de los sistemas

Define como se instala y prueba un equipo nuevo o un programa nuevo, cómo se documentan los cambios de los equipos y la configuración, a quien se debe informar cuando hagan cambios y quién tiene la autoridad para hacer cambios de equipo, programas y configuración.

e) Respaldos y acervos de datos y programas

Define qué sistema de archivos hay que respaldar, cuando hay que hacer los respaldos, cómo se administran los medios que se utilizan para los respaldos, donde se guardan los respaldos fuera de sitio, como se etiquetan los medios y como documentan los respaldos.

f) Manejo de incidentes

Define cómo se manejan las instrucciones, delimita la responsabilidad de cada miembro del equipo de respuesta, indica que información hay que anotar e investigar, a quién hay que notificar y cuándo, determinar quién, cuándo y cómo se hará el análisis posterior del incidente.

g) Escalamiento del problema

Es una colección de recetas para el personal de soporte de primera línea. Define a quién hay que llamar y cuándo, indica que pasos iniciales hay dar y que información inicial hay que anotar.

h) Planes de respuesta a desastres

Un desastre es un evento de gran escala que afecta a grandes secciones de la organización. El plan debe delinear qué acciones hay que tomar para que los recursos críticos sigan funcionando y minimice el impacto del desastre. Debe indicar que hay que tener fuera del sitio y fácilmente disponible para emplearlo después de un desastre. Hay que estratificar el plan para responder a distintos niveles de daños. Definirá si se requieren sitios alternos "calientes" o "fríos". Se debe establecer cada cuando se harán simulacros para probar el plan.

4.1.9 Modelos de Seguridad

Un modelo de seguridad es la presentación formal de una política de seguridad. El modelo debe identificar el conjunto de reglas y prácticas que regulan cómo un sistema maneja, protege y distribuye información delicada (López Barrientos & Quezada Reyes, 2006).

De acuerdo a (López Barrientos & Quezada Reyes, 2006), los modelos se clasifican en:

a) Modelo abstracto: se ocupa de las entidades abstractas como sujetos y objetos. El modelo Bell LaPadula es un ejemplo de este tipo.

b) Modelo concreto: traduce las entidades abstractas en entidades de un sistema real como procesos y archivos.

Además, los modelos sirven a tres propósitos en la seguridad informática:

1. Proveer un sistema que ayude a comprender los diferentes conceptos. Los modelos diseñados para este propósito usan diagramas, analogías, cartas. Un ejemplo es la matriz de acceso.
2. Proveer una representación de una política general de seguridad formal clara. Un ejemplo es el modelo Bell-LaPadula.
3. Expresar la política exigida por un sistema de cómputo específico.

4.1.10 Problemas al implantar las políticas de seguridad

Muchas veces las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito. Pero resulta una labor ardua el convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y la falta de una estrategia de mercadeo de los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para los juguetes de los ingenieros". Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad, que en muchos de los casos lleva a comprometer su información sensitiva y por ende su imagen corporativa.

Ante esta encrucijada, los encargados de la seguridad deben asegurarse de que las personas relevantes entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

En particular, la gente debe saber las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir.

Luego, para que las políticas de seguridad logren abrirse espacio al interior de una organización deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía. De igual forma, las políticas de seguridad deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en su diario hacer, donde se identifiquen las necesidades y acciones que materializan las políticas.

En este contexto, el entender la organización, sus elementos culturales, es decir, la forma en que actúa la gente cuando nadie le dice qué hacer, estableciendo la manera en que los miembros de la empresa deben conducirse, y los comportamientos, los cuales dependerá de su motivación, características personales y del ambiente que lo rodea, nos deben llevar a reconocer claramente las normas de seguridad que tendrán que privar en ese sitio de seguridad necesarias y suficientes que aseguren confiabilidad en las operaciones y funcionalidad de la compañía.

4.2 Procedimientos y Planes de Contingencia

En el mundo de hoy, las organizaciones dependen del procesamiento de datos para el flujo de información esencial, ya que si se quedara sin procesamiento de datos durante dos días, o durante una o dos semanas, las operaciones comerciales podrían limitarse de tal manera que afectaran los activos corporativos, los movimientos comerciales, el servicio a clientes, el flujo de dinero, las oportunidades de inversión y el margen de competencia, toda la organización sería vulnerable en caso de que las operaciones de cómputo no funcionen.

Las amenazas son reales y un desastre puede resultar de diferentes fuentes. Pueden ocurrir desastres naturales, fallas prolongadas de energía eléctrica, incendios, sabotaje y hasta explosión de bombas. Asimismo, es importante comprender que un desastre puede ocurrir de la misma manera que producirse, por ello se debe estar preparado.

Un plan de contingencia o plan de recuperación en caso de desastre es una guía para la restauración rápida y organizada de las operaciones de cómputo después de una suspensión. Específica *quién* hace *qué* y *cómo*. Los objetivos de dicho plan son los de restablecer, lo más pronto posible, el procesamiento de aplicaciones críticas (aquellas necesarias para la recuperación) para posteriormente restaurar totalmente el procesamiento "normal". Un plan de contingencias no duplica un entorno comercial normal (en forma inmediata), pero sí minimiza la pérdida potencial de activos y mantiene a la empresa operando, al tomar acciones decisivas basadas en la planeación anticipada.

Dicho de otra manera, un plan de contingencias es un programa de recuperación de la organización, cabe aclarar que el plan de contingencias no sólo es un problema del área de sistemas, sino de toda la organización.

4.2.1 Definición

Un plan de contingencia es un plan escrito en el que se detallan acciones, procedimientos y recursos que deben usarse durante un desastre que cause destrucción parcial o total de los servicios de computación. En este plan se define qué tareas son críticas, quién es el responsable de todos los aspectos del proceso de recuperación, y cómo va a funcionar la organización mientras los sistemas están siendo reparados o transportados a un nuevo local.

4.2.2 Utilidad del Plan de contingencia

Un plan de contingencia o también llamado plan de recuperación de desastres, permite controlar la situación y realizar las actividades necesarias sin afectar a la información y para ello se debe de tomar en cuenta lo siguiente:

- Disminuirá los efectos de esos desafortunados desastres y permitirá una respuesta rápida, una transferencia del procesamiento crítico a otras instalaciones, y una eventual recuperación.

- Proporcionará a los directivos de una empresa una excelente oportunidad para aliviar o minimizar problemas potenciales que, en un momento dado, podrían interrumpir el procesamiento de datos.

- Deberán tener sentido, ser legibles e indicar todos los aspectos de la función de la cuestión.

- El nivel de detalle para el plan de contingencia, para respaldar la información y para los procedimientos de recuperación, dependerá de la importancia de la aplicación y del tipo de información.

- Se desarrollará un plan de contingencia propio para cada empresa y así cubrirá sus necesidades específicas.

4.2.3 Elementos

El plan de contingencia, es un plan de emergencia y recuperación porque incorpora seguridad física al centro de cómputo, es decir, es un plan formal que describe los pasos a seguir en el caso de presentarse alguna situación de emergencia, con la finalidad de reducir el impacto que pueda provocar el desastre, y posteriormente restablecer las operaciones del procesamiento electrónico de datos en forma tan inmediata como sea posible.

Por lo tanto, el diseño e implementación de un plan de esta naturaleza debe contemplar:

- Los riesgos y los porcentajes de factibilidad de éstos, a los que está expuesta la organización.
- La asignación de responsabilidades al personal, tanto en las actividades que se realizarán durante la emergencia como en las de preparación y las de recuperación.
- La identificación de aplicaciones (sistemas automatizados) de mayor importancia dentro de la producción de datos, para darles la seguridad necesaria.
- La especificación de alternativas de respaldo.
- La definición de procedimientos y políticas a seguir durante el momento de la crisis.
- La definición de medidas y el tiempo previsto para la recuperación.
- La integración de prácticas de mantenimiento, entrenamiento en el plan y pruebas del mismo.

Es importante destacar que un plan de contingencia no evita los desastres, sino que provee los medios para salvaguardar al máximo los recursos del área de procesamiento electrónico de datos y reducir así las posibles pérdidas que resultan de estos desastres.

Una de las claves en el desarrollo de un plan de contingencia estriba en la evaluación de posibles riesgos (posibilidad de ocurrencia), que envuelven el ambiente informático. Sin embargo, es posible prever en un 100% todos y cada uno de los riesgos que acosan nuestra operatividad. Es entonces vital en listarlos y agruparlos con la finalidad de anticipar la mayor parte de ellos y posteriormente establecer el impacto que pueden causar en caso de su materialización

La concepción del plan de contingencia debe tener un alcance tal que permita una completa recuperación de la pérdida eventual, según el tiempo que de antemano se haya considerado para ello. Surge entonces la pregunta ¿qué significa hacer exitoso un plan de contingencia? Consideramos que el éxito de este plan estará en función del tiempo y del costo necesario para restablecer la operación normal de los sistemas de cómputo.

4.2.4 ¿Quién debe escribir el Plan de Contingencia?

Una vez que se ha tomado la decisión de hacer un plan de contingencia, el Director de Sistemas junto con el cuerpo directivo de la empresa determinarán que es lo que más le interesa a la organización y así tomar la decisión si se contrata a un consultor externo para hacerlo o desarrollarlo "en casa". Ambas opciones tienen "pros" y "contras".

De acuerdo a (Rodríguez, 1995), a primera vista, contratar a un consultor externo con muchos años de experiencia en el desarrollo de este tipo de proyectos puede parecer la mejor opción. Algunas de las ventajas son:

- El desarrollo de un plan de contingencia están complicado como cualquier sistema importante (figura 4.1), debido a que en ambos se debe de seguir una serie de pasos ordenadamente para obtener un buen resultado. Por esto requiere de una persona (o un equipo) dedicado exclusivamente al desarrollo de este proyecto.
- Los consultores poseen conocimientos especializados que pueden facilitar el desarrollo más rápido de un buen plan. Un consultor con experiencia sabe cómo se hace un plan de contingencias, además sabe quién es quién dentro de la industria de la seguridad de la información.

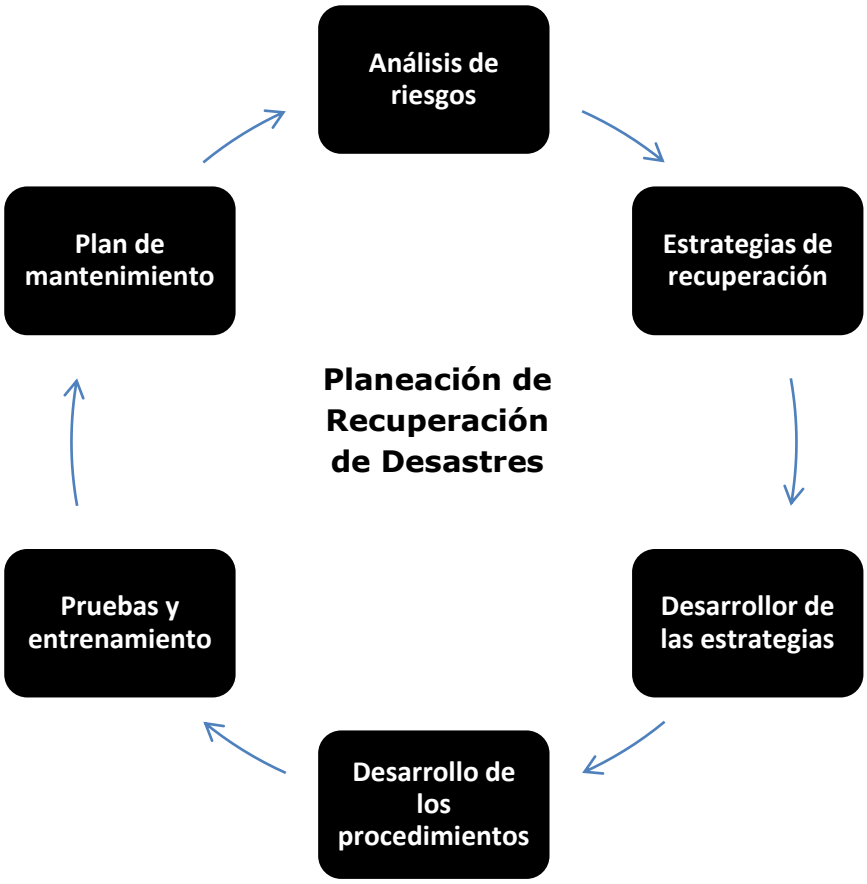


Figura 4.1. Comparación entre el Ciclo de Vida de un Sistema de Información y el de un Plan de Contingencias (Rodríguez, 1995)pág. 170

- Los consultores, al ser externos a la empresa, miran con "ojo nuevo" al proyecto, y se percatan de requerimientos que podrían ser pasados por alto por una persona de la empresa.
- Los planes hechos por consultores, típicamente vienen acompañados de un acuerdo de mantenimiento. Por alguna cuota, el consultor regresará con determinada frecuencia a ayudar en las pruebas, entrenamiento y actualización del plan.

Por su parte la mayor desventaja de contratar consultores especializados en el desarrollo de planes de contingencias es su precio: es muy caro, por lo que muchas empresas no estarían en condiciones de pagarlo.

Por otro lado, si se decide que el plan sea desarrollado "en casa", se tienen las siguientes ventajas:

- El desarrollador del plan de contingencias, al formar parte de la empresa, tendría

un acceso más rápido y completo a la información que necesite.

- El desarrollador del plan, como miembro del área de sistemas (seguramente así será) con ayuda de todos los miembros del personal de sistemas**,** tendrá más facilidad para la realización del inventario de hardware y software, así como para la etapa de clasificación de los sistemas de acuerdo a su importancia y consecuentemente para la definición de los procedimientos de respaldo.

- Podrá conocer todas las medidas de seguridad de la información implementadas en la empresa sin ninguna reserva.

- Puede utilizar el conocimiento que tiene acerca de sus compañeros de trabajo, para tratar de definir quiénes son las personas más adecuadas para la conformación de los diversos equipos de contingencia.

Por lo que respecta a las desventajas de que el plan sea desarrollado por un empleado de la empresa, podemos mencionar las siguientes:

- La persona encargada, en la mayoría de los casos no contará con la experiencia necesaria en el desarrollo de este tipo de proyectos.

- Nuevamente en la mayoría de los casos, a la persona encargada de desarrollar el plan se asignará esta tarea como una adicional a las que ya venía realizando. Es decir, no contará con tiempo completo para dedicarlo a este proyecto. Por lo tanto, el tiempo de desarrollo del plan será excesivamente largo, o bien, será terminado en el límite fijado, pero la calidad del mismo podría no ser completamente satisfactoria.

4.2.5 Metodologías de desarrollo de Planes de Contingencia

A continuación se describen tres metodologías de desarrollo de Planes de Contingencia para Sistemas de Información (Rodríguez, 1995): la de William Toigo, la de Hewlett-Packard y una "Universal" llamada así por sus características.

4.2.5.1 Metodología de William Toigo

Esta metodología consta de ocho etapas. De cada una de ellas se enuncian las principales tareas que la componen.

I. Definición y Arranque

- Definir los objetivos del plan

- Seleccionar la metodología

- Obtener la aprobación de la Dirección
- Diseño de cuestionarios

II. Análisis de riesgos

a) Recolección de datos

- Inventario de hardware, software, aplicaciones, bases de datos y telecomunicaciones.
- Se obtiene el "grado crítico" de los sistemas, tanto desde el punto de vista de los usuarios como de los técnicos.
- Se determina la "tolerancia" a una falla o desastre. En términos prácticos, la tolerancia puede ser expresada como un valor en pesos: es la pérdida de ingresos de la empresa, debida a una suspensión del procesamiento de cierta duración.
- Identificación de amenazas al procesamiento normal. Estas amenazas pueden ser humanas, de error de hardware, de error de red, de tipo lógico y de desastres, ya vistas en el capítulo anterior.

b) Análisis de datos

- Habiendo clasificado el grado crítico de los sistemas, asignado costos a suspensión de funcionamiento del sistema, e identificado amenazas a los sistemas y a la información, resta analizar todos estos datos y formular un conjunto de objetivos específicos para guiar el desarrollo de la capacidad de recuperación. El objetivo es eliminar los riesgos que puedan ser eliminados y minimizar los efectos de los riesgos que no puedan eliminar.

III. Protección de la instalación

En esta sección se discuten varias estrategias comunes de prevención de desastres y de protección que se pueden poner en práctica para proveer la capacidad de evitar desastres:

- Detección de agua
- Protección contra fuego
- Eliminación de contaminantes
- Falla de suministro de eléctrico

- Control de acceso físico

El diseñador del plan de contingencia debe conocer estos temas y su aplicación en la empresa, ya que sin factores que comúnmente organizan desastres.

IV. Almacenamiento fuera del Site[2]

El almacenamiento fuera del *site* incluye el análisis y clasificación de los datos, la revisión de los procedimientos de respaldo existentes (si los hay), la evaluación y selección de un proveedor de espacio de almacenamiento, y la formalización de agendas para el mantenimiento actualizado de datos del *site* externo.

Se requiere que la información correcta (que se usará para reducir el tiempo de suspensión del funcionamiento de los sistemas y sus efectos negativos) sea identificada, para conseguir esto debe realizarse las siguientes acciones:

a) Deben identificarse los sistemas críticos y vitales (este autor clasifica los registros de información como críticos, vitales, sensibles y no críticos, en orden descendente de importancia).

b) Las entradas y salidas de esos sistemas deben ser definidas.

c) También deben almacenarse respaldos de los programas, sistemas y software de la base de datos en producción.

d) Identificar la documentación requerida para restaurar los sistemas e información; esto incluye inventarios, manuales técnicos y de usuario, formas impresas, copias del plan de contingencia, etc.

V. Estrategia de respaldo de Sistemas

En esta etapa nuevamente se hace uso de los resultados del análisis de riesgos. Hay que saber:

a) ¿Qué aplicaciones son críticas o vitales?

b) ¿Cuál es la configuración mínima de hardware para correr los sistemas?

c) ¿Cuántos usuarios tienen los sistemas?

d) ¿Cuáles son los requerimientos de la empresa?

[2] **Site:** Lugar o "sitio" donde está instalado, o puede ser instalado, cierto equipo de cómputo. (Rodríguez, 1995)

Existen muchas estrategias de respaldo de los sistemas de cómputo; debe analizarse cada caso para determinar cuál es la más conveniente.

VI. Estrategia de respaldo de redes

El diseñador del plan de contingencia debe entender las redes de comunicación que están alrededor de los procesadores.

Una actividad preliminar consiste en revisar el análisis de riesgo para identificar dependencias en redes, el grado crítico de los servicios de red y el nivel mínimo de servicio requerido para la continuidad del negocio.

Existen varias opciones para recuperar las redes que han tenido fallas:

a) Para sistemas de comunicación interna:

- Es importante adquirir software apropiado para diagnóstico y reparación de problemas de redes
- En el caso de una falla del conmutador hay dos opciones: (1) instalar suficientes líneas directas para las funciones dependientes de las telecomunicaciones y (2) comprar un segundo conmutador y tenerlo de respaldo.

b) Para equipo periférico de las computadoras:

- Tener hardware redundante almacenado para reemplazo inmediato cuando falla un dispositivo crítico.

c) Para redes de área local:

- Para proteger las redes de área local contra pérdidas catastróficas debidas a la falla de nodos, pérdida de la integridad de los medios de comunicación, o factores relacionados con el software usado para crear y controlar la red.

Además de las fallas de redes, otro escenario de contingencia que puede ser considerado por el diseñador del plan consiste en la falla de la compañía telefónica.

VII. Toma de decisiones en caso de emergencia

Se refiere a tres proyectos fundamentales para la recuperación de emergencias:

- Evacuación
- Recuperación
- Reinstalación de las actividades normales.

Debe tomarse en cuenta las siguientes consideraciones:

a) Es imposible predecir todos los escenarios y tomar todas las decisiones por adelantado; por eso, resulta inútil diseñar procedimientos muy rígidos.

b) Sin embargo, el plan es necesario para coordinar las acciones de recuperación ya que sin él, sería más lenta; y el desastre causaría daños mayores a la empresa.

c) En esta fase debe diseñarse los equipos que llevarán a cabo el plan de contingencia (estos mismos equipos pueden tener diferentes funciones durante la evacuación, la recuperación y la reinstalación de actividades normales).

d) Después de diseñarse, debe formarse los equipos. Así mismo debe hacerse el directorio telefónico de estas personas y de todas las que tengan alguna relación con este plan.

e) Puede diseñarse uno o varios Diagramas de Flujo de Manejo de Emergencias que describan la secuencia en la cual se realizarán las tareas de recuperación.

VIII. Mantenimiento y pruebas del plan

El plan de contingencia es un documento "vivo" y cambiante, por lo que requiere de mantenimiento.

Antes de probar el plan, se debe dar entrenamiento específico a todos los miembros de los equipos de recuperación en las tareas que realizarán en caso de desastre. Los líderes de los equipos, en cambio, deben recibir entrenamiento general sobre todo el plan completo.

a) Los objetivos principales de las pruebas son:

- Asegurar que el plan pueda aplicarse exitosamente recuperando lo que sea posible.
- Las pruebas sirven como una herramienta de auditoría.
- Las pruebas pueden revelar información útil acerca del desempeño de los sistemas a un nivel de emergencia, entre otras cosas.
- Las pruebas son una forma de entrenar y además pueden utilizar sus resultados para corregir el plan o agregarle aspectos no considerados originalmente.

b) Para hacer pruebas:

- Debe establecerse un escenario
- Deben definirse los objetivos de la prueba
- Definirse las reglas

- Designar participantes y observadores
- Documentar los resultados

4.2.5.2 Metodología de Hewlett-Packard

Esta metodología consta de 11 etapas (ver figura 4.2) y de cada una de ellas se enuncian las principales tareas que la componen.

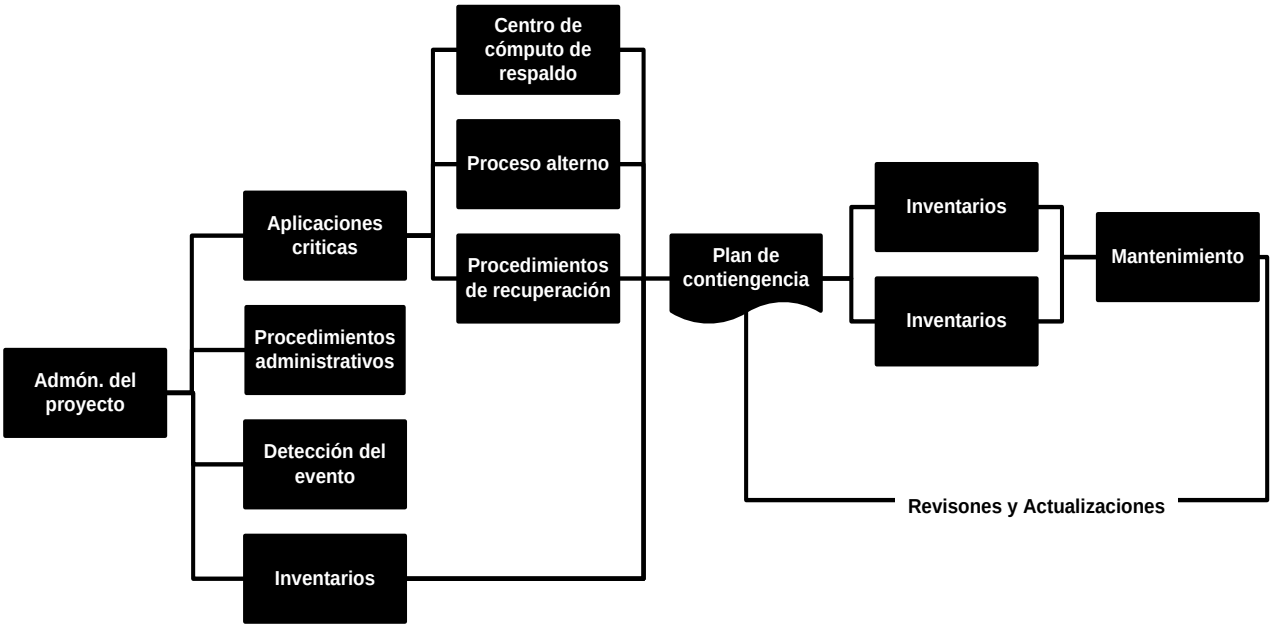


Figura 4. 2 Metodología de Hewlett-Packard para el desarrollo de planes de recuperación de desastres (Rodríguez, 1995)pág. 170

1. Administración de proyectos

a) *Obtener un compromiso preliminar de la Gerencia:* la Dirección de la empresa debe comprometerse a desarrollar el plan de contingencia en caso de desastre, de tal manera que los recursos necesarios puedan ser asignados al proyecto.

b) *Organizar el equipo de desarrollo del plan de contingencia:* identificar a los individuos de la administración, del procesamiento de datos y usuarios, para que participen en la preparación del programa de recuperación.

c) *Auditar el estado de la preparación del plan de contingencia previo (si existe):* algunos procedimientos e información necesarios para el plan de recuperación de desastres posiblemente ya se han desarrollado y puesto en práctica. Sabiendo lo que ya existe y lo que falta por hacer, será posible tomar decisiones más realistas sobre el tiempo y los recursos que debe asignarse al proyecto.

d) *Desarrollar un plan administrativo para el proyecto:* realizar una estimación de la duración de las tareas, asignar recursos y desarrollar un calendario para el proyecto.

e) *Seleccionar las herramientas de documentación:* decidir qué paquete o paquetes se usarán y los procedimientos generales; por ejemplo, quién será responsable de la documentación, cuándo se hará (al concluirlo o durante el desarrollo del plan), ¿existen normas de la empresa para la generación de este tipo de documentos?, etc.

2. Aplicaciones criticas

a) *Establecer prioridades de las aplicaciones:* analizar todas las aplicaciones para priorizarlas e identificar cuáles son críticas. Esta metodología maneja tres categorías: crítica, importante y "todas las demás". Considera que la prioridad de una aplicación se basa en tres factores principales: valor monetario (cantidad de ingresos producidos por la aplicación), limitaciones y prioridades (las aplicaciones pueden ser necesarias por las limitaciones, p. ej. Leyes, regulaciones, contratos; o porque son usadas para reunir las prioridades claves comerciales, p. ej. Servicio a clientes), urgencia de tiempo (la necesidad de ejecutar una aplicación en períodos o frecuencias determinadas).

b) *Especificar prioridades de procesamiento para la recuperación de desastres:* listas las aplicaciones en orden de restauración durante la recuperación. Esta lista sirve para distintos propósitos. En primer lugar, es una herramienta excelente para comunicar las prioridades de procesamiento que serán seguidas en caso de desastre. En segundo lugar, es utilizada en la siguiente actividad, en donde se debe determinar los requerimientos de procesamiento para cada tipo de prioridad. Esto, a su vez, se usa para establecer los objetivos de recuperación y para seleccionar las instalaciones de respaldo apropiadas. Finalmente, es un paso preliminar en el desarrollo de un plan de restauración.

c) *Determinar los requerimientos del procesamiento:* analizar los recursos necesarios para procesar las aplicaciones con prioridad alta, de tal manera que se tenga suficiente capacidad de respaldo. Una decisión clave que debe tomarse es definir cuántos niveles de prioridad van a ser respaldados.

d) *Establecer objetivos de la recuperación de desastres:* especificar el nivel de procesamiento y tiempos de recuperación que se han de lograr en la restauración de desastres menores, mayores y catastróficos.

3. Instalación de respaldo y procedimientos

a) *Seleccionar una localidad externa de almacenamiento (caja de seguridad):* los datos y documentación de respaldo deben almacenarse fuera de la instalación para que sobrevivan, aun cuando exista una destrucción total del centro de cómputo. En esta etapa se debe identificar una o más localidades externas donde se puedan almacenar seguramente los datos y documentación de respaldo.

b) *Determinar el contenido indispensable de la caja de seguridad externa:* identificar los archivos, programas, documentación, materiales, etc., específicos que deban respaldados y mantenidos en un lugar fuera de la instalación.

c) *Especificar procedimientos de almacenamiento y actualización:* determinar el equipo y la capacidad de procesamiento necesaria en la instalación de respaldo.

d) *Identificar los requerimientos del sistema para las instalaciones de respaldo:* determinar el equipo y la capacidad de procesamiento necesaria en la investigación de respaldo. El propósito de esta tarea es investigar qué recursos de cómputo son necesarios en la instalación de respaldo: tiempo, sistemas, periféricos, comunicaciones de datos y otros equipos, para procesar las aplicaciones de determinada prioridad.

e) *Seleccionar una o más de estas instalaciones:* evaluar las instalaciones potenciales de respaldo y elegir una o más para hacer los arreglos necesarios. El plan de contingencia en caso de desastre debe tomar en cuenta un rango de posibilidades desde un desastre menor, tal como una suspensión de cómputo prolongada, hasta un desastre catastrófico que destruya totalmente el centro de cómputo.

f) *Producir una guía de respaldo de la instalación:* una o más instalaciones de respaldo han sido seleccionadas para ser usadas durante la recuperación de desastres. Estas instalaciones se diferenciarán entre sí y del centro de cómputo primario. La información específica de cada una debe documentarse en una guía de la instalación de respaldo.

g) *Identificar al personal de respaldo:* idealmente, el personal del centro de cómputo estará disponible durante un desastre. De cualquier modo, si no está disponible, entonces sus funciones tendrán que ser realizadas por otras personas (el personal de respaldo).

4. Procedimientos y procesamiento alterno

a) *Identificar las aplicaciones críticas que requieran procedimientos del procesamiento alterno:* las aplicaciones críticas son, por definición, aquellas necesarias para la supervivencia de la compañía; el plan de contingencia, en caso de desastre, proporcionan restauración para estas aplicaciones.

b) *Desarrollar los procedimientos de procesamiento alterno:* para las aplicaciones críticas seleccionadas, se debe crear el procedimiento de procesamiento alterno, que pueda usarse en caso de que las instalaciones del centro de cómputo no estén disponibles.

5. Procedimientos de recuperación

a) *Definir equipos de recuperación y sus funciones:* las acciones que deben tomar para efectuar el restablecimiento de un desastre, son llevadas a cabo por equipos de recuperación, cada uno con su propia área de responsabilidad. El propósito de esta tarea es especificar los equipos de recuperación y las funciones de cada uno.

b) *Identificar a los miembros de cada equipo:* nombrar a las personas que servirán en cada equipo de recuperación.

c) *Especificar sus procedimientos:* establecer los pasos de acción que tienen que seguir los líderes y miembros del equipo. Se debe distinguir entre lo que debe realizar el líder y lo que pueden hacer los otros miembros.

6. Procedimientos de detección de eventos

a) *Especificar los procedimientos de emergencia:* los procedimientos de emergencia son las acciones que deben realizarse inmediatamente, en respuesta a un evento dañino o a una situación amenazadora.

b) *Establecer los procedimientos de escalación:* el propósito de esta estos procedimientos es definir la distribución de los pasos y del tiempo que llevan a la declaración de un desastre menor.

7. Procedimientos del equipo de manejo de desastres (EMD)

a) *Identificar a los miembros del Equipo de Manejo de Desastres:* este equipo tiene la responsabilidad de dirigir las operaciones de recuperación y la restauración del procesamiento normal. En esta tarea se debe seleccionar al Gerente de Recuperación de Desastres, al Coordinador del Equipo de Recuperación y a los líderes de los equipos.

b) *Especificar las funciones y los procedimientos del equipo:* el EMD está orientado a los esfuerzos de recuperación dirigidos que siguen a un desastre. Para asegurar que el equipo pueda funcionar efectiva y eficientemente, sus responsabilidades son establecidas en un estatuto formalizado, junto con sus funciones en caso de desastre.

c) *Seleccionar las ubicaciones de los centros de control:* elegir localidades internas y externas para usarse como centro de control. Las operaciones de recuperación de desastre se deben dirigir desde un centro de control y su propósito puede establecer una sola palabra: comunicación. Cuando se declara un desastre y durante las operaciones subsecuentes de restablecimiento, todos los equipos y el personal estarán en contacto continuo con el centro de control. Por esto, es importante que todos sepan dónde estará el "centro nervioso" durante una emergencia.

d) *Listar los recursos del centro de control:* el centro de control debe estar bien equipado, especialmente con herramientas de comunicaciones (teléfonos, radios,

directorios públicos, etc.). Una lista de verificación de los recursos y registros necesarios en el centro de control activado, minimizará el tiempo necesario para hacerlo funcionar.

e) *Realizar un inventario del material necesario para las aplicaciones críticas:* la evaluación del daño y del impacto son actividades clave de la administración de desastres porque proporcionan la información necesaria para la toma de decisiones. Un inventario completo y categorizado (recopilado en la siguiente fase) puede servir como base para la evaluación del daño y del impacto.

8. Inventario

a) *Llevar un inventario de todos los recursos del procesamiento de datos:* el inventario debe dividirse en categorías y después subdividirse en categorías dentro de esas categorías, para hacer más fácil la recopilación, la actualización y el uso. Se deben recopilar listas de hardware, software, equipo, materiales y otros recursos usados para el procesamiento de datos.

b) *Listar a los distribuidores de los recursos críticos:* es necesario recopilar información de distribuidores, por lo menos de cosas utilizables en el procesamiento de aplicaciones con prioridad alta.

9. Entrenamiento

a) *Diseñar un plan completo para el entrenamiento de recuperación de desastres:* es necesario un programa general de entrenamiento para asegurar que las personas correctas obtengan el tipo de adiestramiento adecuado. Debe entrenarse a cada persona en las funciones que tiene asignadas en el plan de contingencia, esto es, en las funciones que desempeñará el equipo o equipos de recuperación a que pertenezca. Por lo menos debe incluir objetivos, programas, calendario y administración.

b) *Desarrollar actividades específicas de entrenamiento:* el plan de instrucciones de cada una de las actividades en el programa de adiestramiento debe seguir cualquier formato acostumbrado o conveniente. Los planes deben ser específicos, claros y completos. Los objetivos deben ser específicos y describir lo que los estudiantes podrán hacer como resultado del adiestramiento.

c) *Desarrollar técnicas y herramientas de evaluación:* el entrenamiento tiene como función primaria el desarrollo del conocimiento y la habilidad. La técnicas de evaluación deben dirigirse para contestar tres preguntas básicas: (1) ¿son capaces los estudiantes de llevar a cabo sus responsabilidades?, (2) ¿cómo puede mejorarse el entrenamiento? Y (3) ¿cómo puede mejorarse el plan de contingencia?

10.Pruebas

a) *Diseñar un programa completo de pruebas del plan de contingencia:* las pruebas del plan de contingencia en caso de desastres deben llevarse a cabo de manera cuidadosa y sistemática. Los puntos clave para que deben incluirse en el diseño de este programa son: objetivos, políticas y guías, responsabilidad gerencial de las pruebas, especificación de las pruebas.

b) *Desarrollar planes para pruebas específicas:* escribir un plan para cada prueba que ha de ser conducida.

c) *Desarrollar técnicas y herramientas de evaluación de las pruebas:* la pruebas del plan de contingencia proporcionan información importante sobre la adecuación del plan y del entrenamiento. Por ello, esta tarea está dedicada a las técnicas y herramientas que se usarán para reunir esta información.

11.Mantenimiento

a) *Asignar responsabilidades para la administración y el mantenimiento del plan de contingencia:* el mantenimiento del plan de contingencia involucra varias funciones:

- Recibir y controlar información de las revisiones necesarias
- Mantener una lista de distribución de las copias del plan y controlar su circulación
- Mantener la historia de revisiones del plan
- Asegurar que las revisiones se lleven a cabo puntualmente
- Distribuir las actualizaciones como sea necesario
- Coordinar el ciclo de revisión con los calendarios de entrenamiento y de pruebas
- Coordinar con los auditores el calendario de revisión y mantenimiento.

b) *Establecer procedimientos y calendarios de revisión y mantenimiento:* los propósitos de esta tarea son proporcionar un calendario para la revisión regular y sistemática del contenido del plan de contingencia en caso de desastre y definir un procedimiento para los cambios sugeridos.

c) *Crear listas de distribución y políticas para el programa de recuperación:* el plan de contingencia contiene mucha información sensible sobre las operaciones de cómputo y comerciales de la compañía; por ejemplo, aplicaciones críticas, ubicación de la caja de seguridad, arreglos para instalaciones de respaldo, etc. Es por esto que la distribución del plan de recuperación es un punto que merece una consideración cuidadosa.

4.2.5.3 Metodología "Universal"

Independientemente de la metodología que se elija para el desarrollo del Plan de Contingencias, o que se desarrolle una propia, existen ciertas constantes que deben aparecer en cualquier plan de este género. En el marco teórico que se presenta a continuación, se proporcionan estos elementos; con ello se puede desarrollar una metodología propia o adaptar una existente. Además, podemos denominar a esta metodología como "universal" porque con ella se puede desarrollar planes de contingencia no sólo para sistemas, sino para cualquier otra área o empresa de cualquier giro o tamaño que resida en cualquier lugar.

1. Conceptualización del Fenómeno de Desastre

I. La producción de Desastres

El desastre, en términos generales, se considera como un evento, frecuentemente concentrado en tiempo y espacio, en el cual la sociedad una parte de ella sufre severos daños, de gran magnitud y extensión, e incurre en pérdidas para sus miembros, de tal manera que su estructura social ya administrativa se desajusta, impidiendo la realización de sus actividades esenciales, afectando su funcionamiento y operación normales, perjudicando crucialmente su capacidad de afrontar y combatir la situación de emergencia.

Se pueden identificar dos sistemas interactuantes responsables por la problemática de desastres. Por un lado, el sistema perturbador (SP), que corresponde a aquel capaz de generar o producir calamidades y, por el otro, el sistema afectable (SA), integrado por el hombre (personal), bienes (hardware, software, información, comunicaciones), el medio ambiente (centro de cómputo, aire acondicionado, etc.) y servicios necesarios para subsistencia (energía eléctrica, servicios portadores), expuestos a las calamidades, las cuales pueden provocar daños en éste y, consecuentemente el desastre.

El análisis de la relaciones entre el SP y el SA muestra que las calamidades como productos del SP están interrelacionadas entre sí, en tal forma que la ocurrencia y características de una pueden verse modificadas por las otras. Esta interrelación se denomina retroalimentación SP-SP.

Así mismo, el estado del sistema afectable puede activar o reprimir la producción de calamidades por el SP. Esta interrelación se denomina retroalimentación SA-SP.

Finalmente, se observa situaciones cuando el sistema afectable influye sobre su propio comportamiento y estado, de tal manera que se agrava o disminuye el desastre, o se abandona o fortalece el estado normal; por ejemplo la interrupción del servicio eléctrico implica la suspensión del servicio de procesamiento de datos. Este tercer tipo de interrelación se denomina retroalimentación SA-SA.

II. La regulación

Para disminuir la ocurrencia de los desastres, surgen dos posibilidades: una, de intervenir en el proceso de producción de las calamidades, con el fin de impedir o disminuir su ocurrencia, y la otra, de cambiar el estado y función del sistema afectable para disminuir las consecuencias del impacto desastroso (figura 4.3).

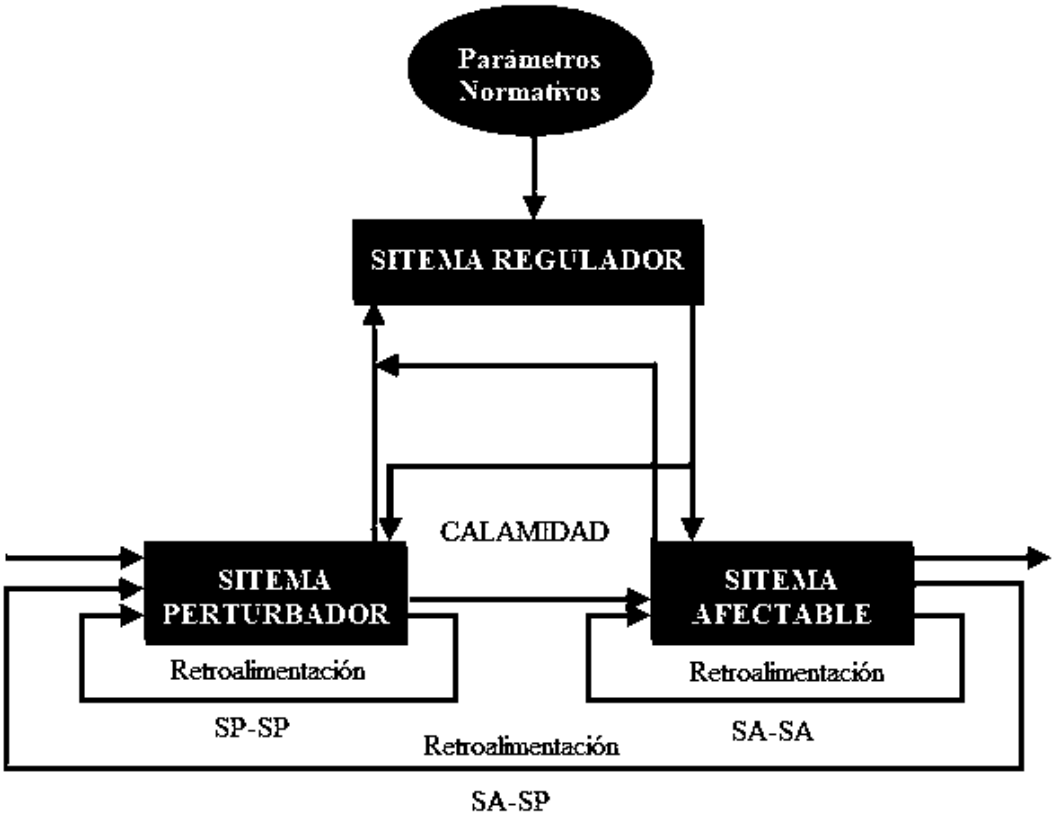


Figura 4.3 El Control de desastres (Rodríguez, 1995) pág.189

Es necesario enfrentar y combatir las situaciones de emergencia durante los desastres, buscando salvar vidas e información de datos e impedir la extensión del desastre, siendo éste el objetivo del rescate o auxilio. En la siguiente fase, llamada "de retorno", con el eventual mejoramiento de la situación, se trata de reconstruir y mejorar el sistema afectado, planteando el objetivo de recuperación. Ambos se engloban en el objetivo general de restablecimiento (figura 4.4).

- Reducción de Riesgos o Protección	**Prevención:** impedir o disminuir la ocurrencia de calamidades
	Mitigación: disminuir los efectos de los impactos de calamidades
	Auxilio o Rescate: salvar vidas o bienes. Estabilizar servicios estratégicos y de soporte de la vida e impedir la extensión del desastre.
- Restablecimiento	**Recuperación:** reconstruir y mejorar el sistema afectable

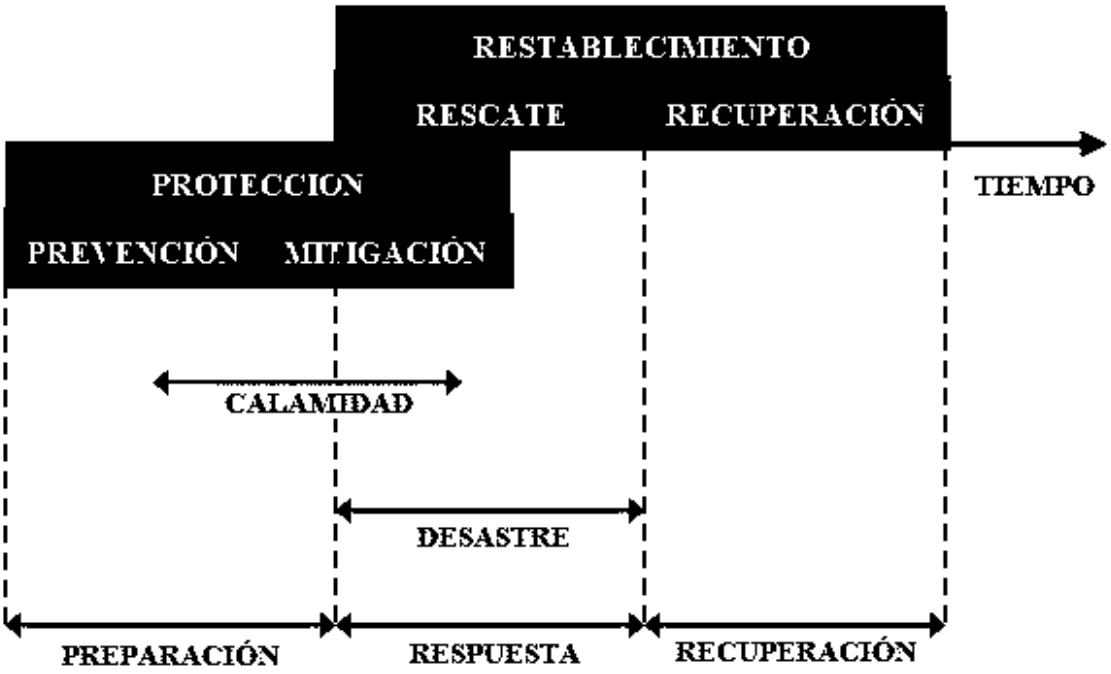


Figura 4.4 Objetivos de Control de Desastres (Rodríguez, 1995) pág.190

El sistema regulador tiene que alcanzar todos estos objetivos, apoyándose en la información sobre el estado actual de los SP y SA, y a través de la previsión, toma de decisiones y de la ejecución de una multitud de diversas acciones, tanto antes como durante y después del desastre, organizadas en el tiempo y apoyadas con recursos correspondientes, por medio de equipos con responsabilidades bien definidas.

2. Elementos fundamentales del marco conceptual

I. Estudios básicos del sistema perturbador

El estudio del sistema perturbador (SP) se inicia con la identificación, definición y clasificación de las calamidades potenciales que puede producir. Tradicionalmente se ha distinguido por las llamadas naturales y de origen humano.

Los fenómenos naturales que provocan desastres pueden ser de origen geológico y de origen hidrometeoeológico. Los fenómenos naturales que causan desastres de origen humano son principalmente los llamados socio-organizativos.

Sin embargo, hay ciertas calamidades cuyo origen está relacionado tanto con los procesos naturales, como con las acciones humanas que las provocan. En este sentido, las calamidades físico-químicas y sanitarias son de origen mixto.

Un factor crucial en el desarrollo del marco conceptual para conocer, explicar y controlar las calamidades, constituye la definición de sus características, así como la descripción y estimación de sus impactos.

En relación con los impactos, que constituyen la más importante característica de la calamidad, se define dos tipos básicos, los primarios y los agregados.

Entre los primarios se distinguen, según su forma de manifestación, los mecánicos, térmicos, químicos, eléctricos, radiológicos, bacteriológicos y psicológicos, mientras que los agregados se dividen en biológicos, productivos, sociales y políticos.

II. Estudios básicos del sistema afectable

El estudio de los sistemas afectables empieza con la consideración de que los asentamientos humanos, por su propensión a las diversas calamidades y debido a la alta densidad poblacional y complejidad de sus servicios, resultan con mayores pérdidas humanas, daños materiales y otras consecuencias desastrosas.

Para estimar el riesgo latente en un sistema afectable, es necesario conocer el estado y vulnerabilidad de cada uno de los subsistemas que lo componen.

En este sentido, el estado de un sistema se define como una característica global que está determinada por un conjunto de valores en que se encuentran los parámetros relevantes para su funcionamiento en un momento dado. Se distinguen cuatro tipos de estado:

- *Estado normal de un sistema*: se presenta cuando su funcionamiento garantiza el logro de su finalidad.
- *Estado insuficiente de un sistema:* ocurre cuando, en su funcionamiento normal, se presenta alguna alteración no significativa que hace vulnerable al sistema.
- *Estado de desastre de un sistema:* aparece cuando su funcionamiento falla, es decir, cuando se presenta una alteración significativa y con tendencia a crecer; se identifica por daños de distintos tipos: humanos, materiales, productivos, sociales, ecológicos, etc.
- *Estado de retorno de un sistema:* se caracteriza por la disminución de la alteración y por la recuperación progresiva de su funcionamiento normal.

Para determinar el estado en que se encuentra un sistema, es necesario el conocimiento de los rangos permisibles para cada uno de los parámetros que caracterizan al mismo.

Una característica integral del sistema es la vulnerabilidad, considerada como medida de susceptibilidad al daño y la intensidad del impacto. Su forma típica se muestra en figura 4.5. Se observa que la primera parte de la curva se refiere a los niveles de intensidad relativamente bajos que normalmente se absorben por el propio sistema sin sufrir daños sensibles; por su parte, la última corresponde al caso de su destrucción o inutilización completa.

El concepto de vulnerabilidad de un sistema es general, por lo que su evaluación puede realizarse tanto a través de la información histórica como del conocimiento de los mecanismos y estructura interna del sistema. En la segunda opción, la evaluación de la vulnerabilidad de un sistema complejo se realiza a través del análisis de sus estructuras y de la estimación de las vulnerabilidades de los subsistemas, partes, componentes y elementos que lo integran; por lo que es posible identificar los que son críticos y buscar consecuentemente las medidas para disminuir su vulnerabilidad y, por ende, la del sistema en su totalidad.

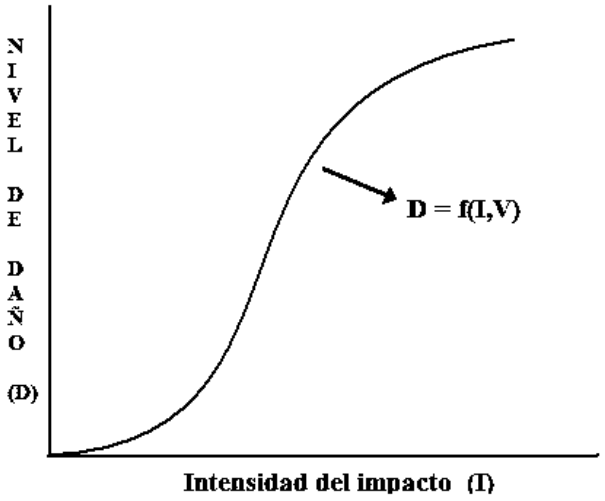


Figura 4.5 Curva típica de vulnerabilidad (Rodríguez, 1995) pág. 195

III. Sistema regulador

En el caso del proceso de control de desastres surgen dos objetivos generales: uno, encaminado a reducir los riesgos, que integra los objetivos de prevención y de mitigación, antes de la ocurrencia del desastre; el otro, atender la situación de emergencia, durante la respuesta, que engloba los objetivos de auxilio y de recuperación.

La reducción de riesgos, es decir, de los probables daños que pueden producir las calamidades en el SA, implica la necesidad de determinar los fenómenos destructivos, a los cuales está propenso el SA, y de estimar sus características relevantes. Posteriormente, implica la necesidad de intervenir en los mecanismos de su producción, en el SP, con el fin de prevenir la concurrencia y disminuir sus impactos.

Así mismo el riesgo depende de la vulnerabilidad del SA, que a su vez, se define por la vulnerabilidad de sus componentes y elementos. Es por ello que la reducción de riesgos también depende, en gran parte, de la eficiencia en la disminución de la vulnerabilidad, por medio del reforzamiento estructural del SA o de la modificación adecuada de su funcionamiento.

El otro objetivo general, el de restablecimiento, implica la necesidad de realizar los preparativos durante la situación normal para asegurar el logro de los objetivos de rescate y recuperación en caso de desastre.

Los preparativos contemplan el establecimiento de la organización relevante, incluyendo los equipos de recuperación de emergencias, la integración y capacitación de su personal, la elaboración de planes y programas de acción, realización de los simulacros pertinentes así como el suministro de dispositivos, equipos y materiales necesarios para su operación en caso de desastre. Asimismo, debe tomarse en cuenta a los cuerpos especializados de rescate y atención de emergencias de la localidad, así como los planes de protección civil y de respuesta a desastres.

El rescate o auxilio constituye el objetivo medular de la fase de respuesta y está integrado por las once funciones principales que se listan a continuación (Rodríguez, 1995):

- *Alerta.* Avisa tanto a los probables afectados, como a los responsables de la atención de emergencia.
- *Reconocimiento de daños.* Conocer y evaluar el estado actual de daños.
- *Concreción del plan de emergencia.* Revisar constantemente el plan de atención de emergencias, de acuerdo con la situación presentada.
- *Coordinación de auxilio.* Asegurar la congruencia, compatibilidad y sincronización de los esfuerzos de los diversos organismos.
- *Seguridad.* Orientada a proteger no solo la integridad física sino también el patrimonio (recursos informáticos, hardware y software).
- *Rescate.* Contempla la búsqueda y salvamento de los recursos.
- *Servicios estratégicos, equipamiento y bienes.* Consiste en restablecer el funcionamiento de los servicios básicos afectados.
- *Salud.* Proporcionar y coordinar la atención médica al personal afectado durante el desastre.

- *Aprovisionamiento.* Realiza, administra y coordina el acopio, distribución y control de los elementos requeridos para sustentar las actividades básicas.

- *Comunicación social de emergencia.* Busca logar la participación de todo personal y crear una atmósfera de confianza.

- *Reconstrucción inicial y vuelta a la normalidad.* Recuperar las condiciones de normalidad, rehabilitando el funcionamiento de los sistemas afectados.

El último objetivo, el de recuperación, concluye la fase de emergencia y corresponde al estado de retorno; es uno de los más importantes, debido a que su inadecuado planteamiento puede agravar el desastre y producir consecuencias mucho más graves que el fenómeno destructivo por sí mismo.

4.2.5.4 Metodología para el Desarrollo de Planes de Atención de Emergencias

El desarrollo de los planes de atención de emergencia constituye una parte esencial de cualquier programa de control de desastres en un sistema, ya que proporciona una herramienta de apoyo a la toma de decisiones para atender las emergencias, en conjugación con los planes de otros sistemas externos.

Los planes de atención de emergencia tienen que contemplar una serie de actividades previstas a realizarse para resolver las diversas situaciones de emergencia que se presentan en un sistema como resultado de los impactos de una calamidad. A continuación se presenta la concreción y adaptación de planeación para la atención de emergencias.

Se distinguen cuatro etapas (Rodríguez, 1995):

1. *Diagnóstico:* plantea los problemas actuales y futuros.

2. *Prescripción:* busca y selecciona una de las soluciones.

3. *Instrumentación:* transforma la solución en actividades o programas que garantizan su logro.

4. *Control:* pone en práctica los programas y evalúa sus resultados, a fin de realizar ajustes y adaptaciones que mejoren la ejecución de las acciones.

La elaboración de los planes de atención de emergencias no debe pretender dar como resultado un producto terminado, ya que esto conduciría a un enorme gasto de tiempo y esfuerzo, para lograr finalmente un plan que de todas maneras no sería perfecto. Por lo tanto, para la adaptación del esquema general de planeación, se tiene como propósito buscar un plan preliminar, una primera aproximación, susceptible de ser mejorado y adaptado fácilmente de acuerdo con las nuevas experiencias y/o las condiciones del sistema y su entorno.

La adaptación del esquema general del proceso de planeación se realiza de la siguiente manera:

a) *La etapa del diagnóstico* se interpreta como la identificación de las posibles situaciones de emergencia, que se presentan en un sistema ante la ocurrencia de una calamidad. La identificación de estas situaciones debe incluir su descripción y la determinación de los límites mínimo y máximo de la gravedad de la emergencia.

b) *La etapa de prescripción* se interpreta como la especificación de alternativas de solución a las soluciones de emergencia, las que, de acuerdo con los estudios desarrollados, deben estar orientadas a brindar el apoyo a la realización de la atención de emergencia, así como a impedir la extensión del daño.

c) *La etapa de instrumentación* se interpreta con la trasformación de las soluciones para cada una de las determinadas situaciones de emergencia en un conjunto de elementos específicos que constituyen un programa. Estos elementos deben normar los criterios del personal responsable de decidir la selección de acciones imprevistas, así como el establecimiento del conjunto de alternativas de acción del decisor y las acciones de los organismos involucrados.

d) *Finalmente, la etapa del control* se interpreta como la estimación de la eficiencia y adaptación del plan, a través del conocimiento de los resultados de su ejecución, con el fin de corregirlo sistemáticamente de acuerdo con las condiciones cambiantes internas y del entorno.

Una vez establecidas las posibles situaciones y fijados los límites de la gravedad de las emergencias, se debe plantear los objetivos y metas de la atención de emergencias.

Estos objetivos y metas constituyen la base normativa de los criterios que deben utilizarse al aplicar el plan, ya que es posible que durante su ejecución surjan alternativas o necesidades no previstas.

4.3 Perfiles de Protección

Los Criterios Comunes (CC) contienen el criterio de evaluación que permite a un evaluador informar si un Perfil de Protección (PP) es completo, consistente y técnicamente válido.

Un PP debe presentarse como un documento orientado al usuario, y se ajustará al contenido de los requerimientos descritos en CC.

La estructura que se presenta a continuación, es la forma en cómo se ha construido la metodología de perfiles de protección y la cual se basa en el seguimiento de los puntos contemplados de manera general en la figura 4.6.

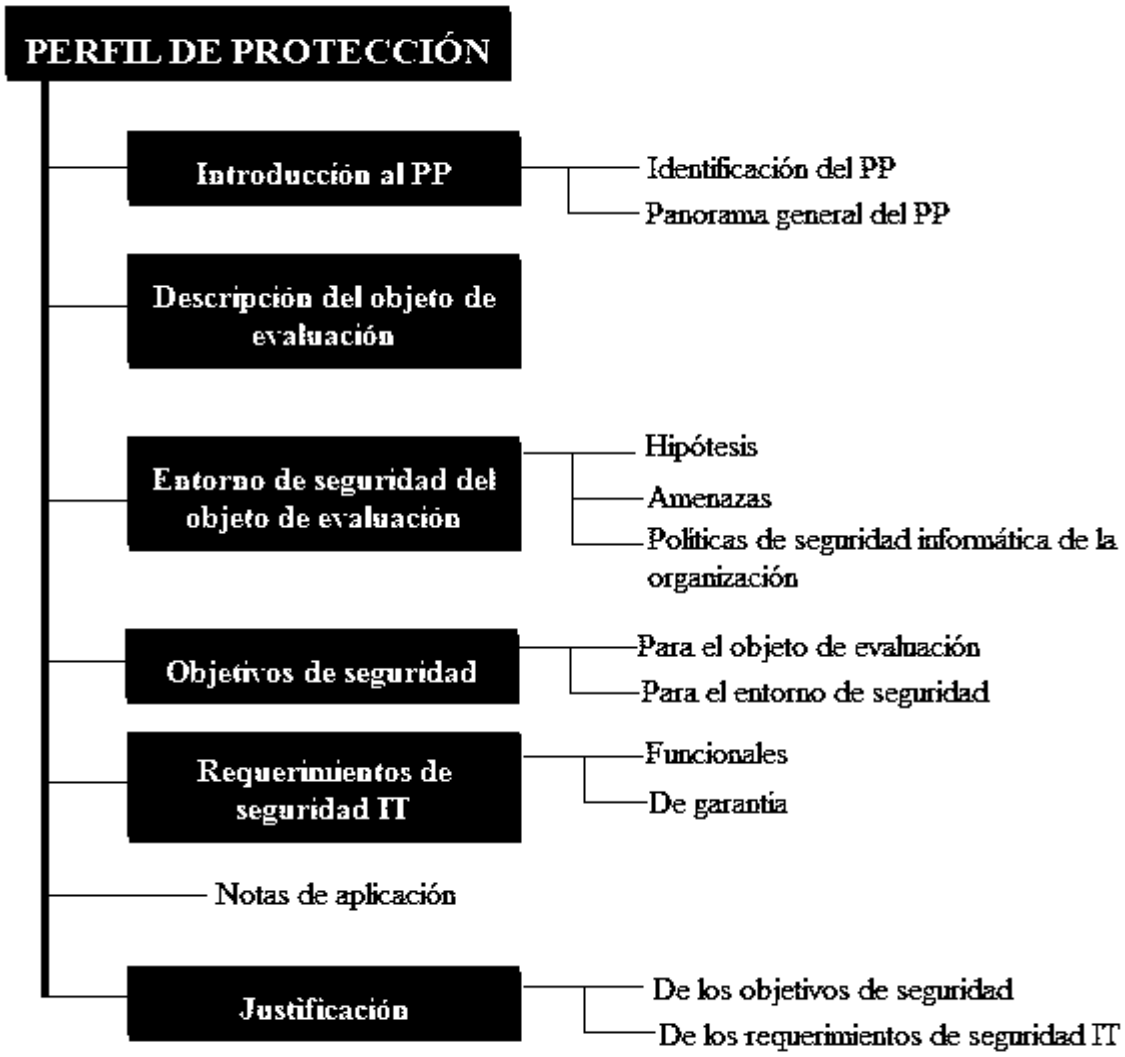


Figura 4.6 Contenido del perfil de protección

a) Introducción

Contendrá el documento administrador y un panorama del PP como se indica a continuación:

1. El *documento administrador* se refiere a la identificación del PP que proporcionará la etiqueta y la información descriptiva necesaria para identificar, clasificar, registrar y cruzar referencias en un PP.

2. El *panorama del PP* recopilará el PP en su forma narrativa, será lo suficiente detallado a fin de que los lectores de la introducción puedan determinar sin lugar a dudas si el PP es de interés para la organización.

Con base a lo anterior podemos decir que la introducción es:

- Resumen ejecutivo (lo que el dueño o directivo de la organización tiene que ver)
- Explicación clara y concisa del problema de seguridad que hay que resolver y de cómo el esquema de seguridad dará solución al mismo.
- Síntesis de la información consistente con el contenido técnico del PP.

b) Descripción del objeto de evaluación

En esta parte del PP se describe al objeto de evaluación a fin de entender sus requerimientos de seguridad.

La descripción:

- Añade detalles que complementan la información que aparece en la Introducción.
- Va dirigido principalmente al técnico administrador.
- Incluye una descripción funcional, la cual es más detallada y va más allá de una descripción de las características de seguridad.
- Contiene una descripción de la frontera del objeto de evaluación, informando de manera muy clara qué es lo que está contenido en el objeto de evaluación, y qué es lo que está fuera de él.
- Debe ser consistente técnicamente.

c) Entorno de seguridad

Se deben describir los aspectos de seguridad del entorno en el cual se pretende utilizar el objetivo de evaluación y la forma como se espera éste sea empleado, de manera que debe incluir:

1. Una descripción de las *hipótesis.*
2. Una descripción de las *amenazas.*
3. Una descripción de las *políticas de seguridad organizacional.*

En el entorno de seguridad:

- La descripción se enfoca principalmente a las necesidades del usuario y con ello facilita la definición de requerimientos.
- El análisis considera los diversos factores con los que interactúa.
- Su análisis hace explícitas las hipótesis que se plantea al desarrollar el PP y las expectativas sobre el entorno que no se resolverán en otros ámbitos.
- Su análisis identifica las amenazas a las que está expuesto el objeto de evaluación

y determina las políticas de seguridad que deberán operar para resguardar el entorno.

d) Hipótesis

A través de las hipótesis se mostrarán los aspectos de seguridad del entorno, para lo cual se debe incluir: información acerca de cómo se pretende utilizar el objeto de evaluación, información acerca del entorno de uso objeto de evaluación. Así:

- Con base en el entorno y su interacción con diversos elementos, se establecen las hipótesis, esto es, la forma en que se considera debería comportarse de manera segura el objeto de evaluación.

- Deben identificarse las hipótesis y el alcance de los requerimientos relacionados con el entorno físico, el personal, los procedimientos y la conectividad.

- Debe evitarse, en la medida de lo posible, incluir detalles de las funciones de seguridad en la definición de hipótesis.

- Debe asignarse una etiqueta o nombre a cada hipótesis para facilitar las referencias.

e) Amenazas

Se consideran todas aquellas que atentan contra los bienes de la organización y contra las cuales se requiere protección, cada amenaza será descrita en términos den un agente identificado como una amenaza, un ataque y del bien que es el sujeto del ataque.

El apartado correspondiente a amenazas contendrá:

- Las que sean importantes en términos de desarrollo de los requerimientos.

- Las que los usuarios del objeto de evaluación y quienes hagan uso del esquema de seguridad quieran ver explícitamente todas en cuenta.

- Las amenazas que sean relevantes, determinando cuáles son los bienes que requieren protección, contra qué métodos de ataque o contra qué eventos indeseables hay que protegerlos, y quiénes o cuáles son los agentes amenazadores.

- Las descripciones de las amenazas de forma explícita, especificando claramente el origen de la amenaza, que bienes están bajo ataque y cuál es el método de ataque.

- Las descripciones de las amenazas de manera concisa, evitando el traslape de éstas.

- Las amenazas que pongan en riesgo a los bienes informáticos, en lugar de los ataques que se basen en debilidades o fallas de la implementación del objeto de evaluación.

- Una etiqueta o nombre para cada amenaza a fin de facilitar las referencias.

f) Políticas de seguridad de la organización

A través de las políticas de seguridad se identificará, y si es necesario explicará, cualquier enunciado de política de seguridad organizacional y las normas con las cuales el objeto de evaluación debe cumplir; con lo que se pretende:

- Determinar las políticas de seguridad informática para la organización, así como los requisitos que no se puedan satisfacer sólo mediante el estudio de las amenazas.

- Determinar las políticas como conjuntos de reglas que deben ser implementadas por el objeto de evaluación.

- Asignar una etiqueta o nombre a cada política para facilitar las referencias.

Con el diagrama mostrado en figura 4.6 se observa que después de llevar a cabo la introducción al PP que se pretende desarrollar, así como la descripción del objeto, la primera parte del análisis se refiere al estudio del *entorno de seguridad* en el cual se encuentra el objeto de evaluación, y esta primera parte del análisis se muestra gráficamente en la figura 4.7.

Figura 4.7 Análisis del entorno de seguridad

g) Objetivos

El informe de los objetivos de seguridad definirá los objetivos de seguridad para el objeto de evaluación y su entorno. Se identificarán las siguientes categorías de objetivos:

1. *Objetivos de seguridad para el objeto de evaluación:* deberán estar claramente documentados y referidos a los aspectos de las amenazas identificadas para que puedan ser contrarrestadas por el objeto de evaluación y por las políticas de seguridad organizacional.

2. *Objetivos de seguridad para el entorno:* deberán estar claramente documentados y referidos a los aspectos de las amenazas identificadas no contrarrestadas completamente por el objeto de evaluación y las políticas de seguridad organizacional o hipótesis no completamente reunidas.

Los objetivos de seguridad indicarán:

- Cómo se hace frente a las amenazas y a las políticas desde el punto de vista de las hipótesis.
- La naturaleza de los requerimientos.
- El grado de efectividad esperado.
- El enfoque particular de cada objetivo.
- elación entre el objetivo, las políticas y las amenazas; la cual puede ser: uno a uno, uno a muchos, o muchos a uno.
- Un objetivo de seguridad para cada requerimiento funcional, principal si es qué éstos se conocen, a fin de facilitar el mapeo de los objetivos a los requisitos.
- Cualquier objetivo de seguridad que se deba cumplir en el entorno.
- Cualquier responsabilidad de procedimientos que se refiera a la administración y uso de medidas de defensa del objeto de evaluación como objetos de seguridad, y debe incluir hasta qué punto se satisfagan los requerimientos.
- El tipo de cada objetivo, esto es, si es de tipo preventivo, detectivo o correctivo.
- Una etiqueta o nombre a cada objetivo para facilitar las referencias.

Como se observa, para establecer los objetivos de seguridad (figura 4.8) ha sido necesario considerar los resultados obtenidos del análisis del entorno de seguridad (hipótesis, amenazas y políticas de seguridad), a través de un proceso cíclico y de refinamiento.

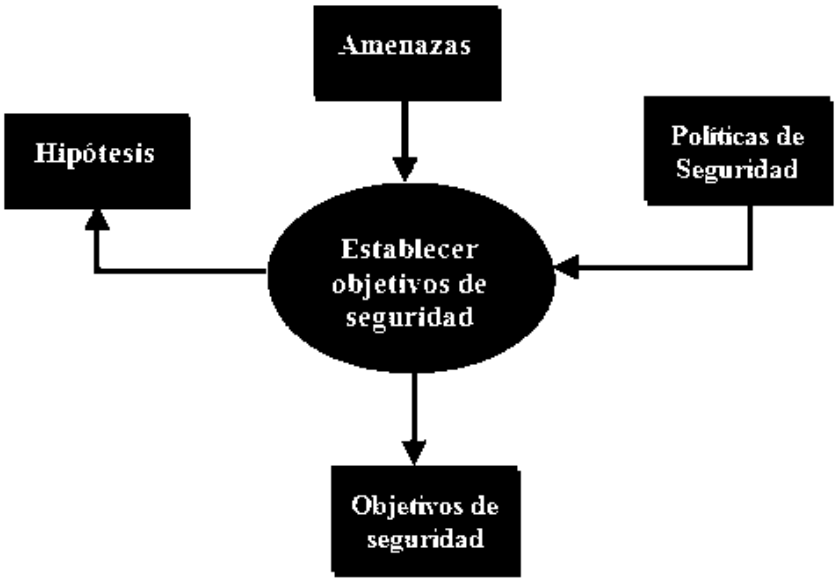


Figura 4.8 Determinación de objetivos de seguridad

h) Requerimientos

En esta parte del PP se definen detalladamente los requerimientos de seguridad IT que deberán ser cubiertos por el objeto de valuación o por su entorno, para ello será necesario realizar una valoración de los bienes, a fin de determinar el nivel de seguridad y de garantía necesarios y seleccionar los requerimientos de garantía de la tecnología de la información con base en el valor de los activos que se desean proteger; para definir los requerimientos de seguridad de IT necesarios , hay que considerar los catálogos de requerimientos incluidos en CC (figura 4.9).

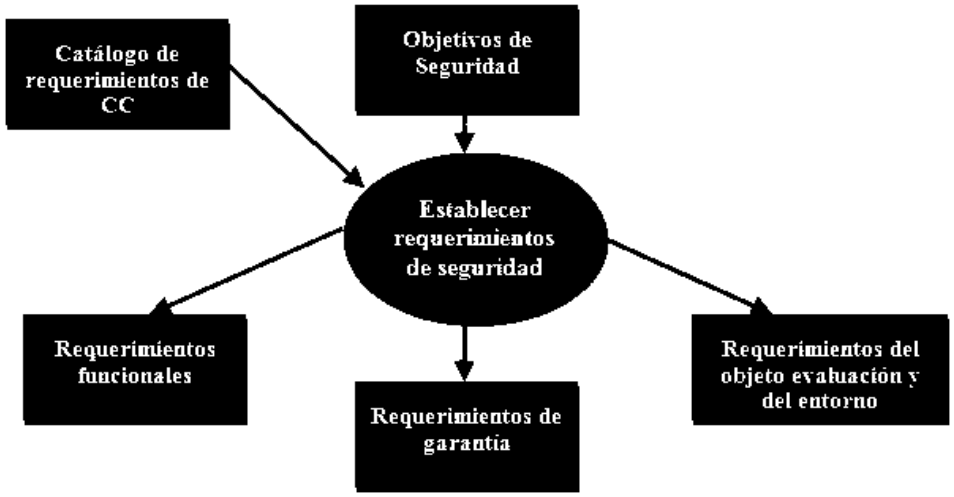


Figura 4.9 Determinación de objetivos de seguridad

El informe de los requerimientos de seguridad definirá los requerimientos que le permitan al objeto de evaluación y a su entorno funcionar seguramente, así como aquellos que le permita al entorno garantizar su seguridad, y se definirán en dos vertientes: la primera se refiere todo aquello que requiera el objeto de evaluación a fin de que éste opere (funcione) de manera segura, a este tipo de requerimientos se le denomina *requerimientos funcionales*; la segunda se refiere a aquello que garantice que el objeto de evaluación es seguro y por lo tanto el usuario de éste lo considere confiable, a este tipo de requerimientos se les denomina *requerimientos de garantía.*

i) Justificación

La justificación debe realizarse considerando dos aspectos fundamentales: *los objetivos de seguridad y los requerimientos de seguridad*; el primero demostrará que el conjunto de los objetivos de seguridad es fácil de seguir para todos los aspectos identificados en el entorno de seguridad del objeto de evaluación, y que es conveniente cubrirlos, y el segundo demostrará que será de gran utilidad reunir el conjunto de requerimientos de seguridad, y que es fácil de seguir para alcanzar los objetivos planteados.

j) Definición de la arquitectura

Se seleccionan los mecanismos y herramientas necesarios y se lleva a cabo su implementación, (figura 4.10), para lo cual es imprescindible:

- Diseñar la arquitectura de seguridad basada en los requerimientos identificados.
- Llevar a cabo la selección de las herramientas que logren los objetivos planteados, hagan cumplir las políticas de seguridad y contrarresten las amenazas identificadas.
- Buscar soluciones que protejan el objeto de evaluación en particular, así como el software, el hardware y el fireware asociados al entorno de seguridad, con lo que las compañías y proveedores de servicio están comprometidos a fin de detener, evitar y contrarrestar ataques de seguridad IT.

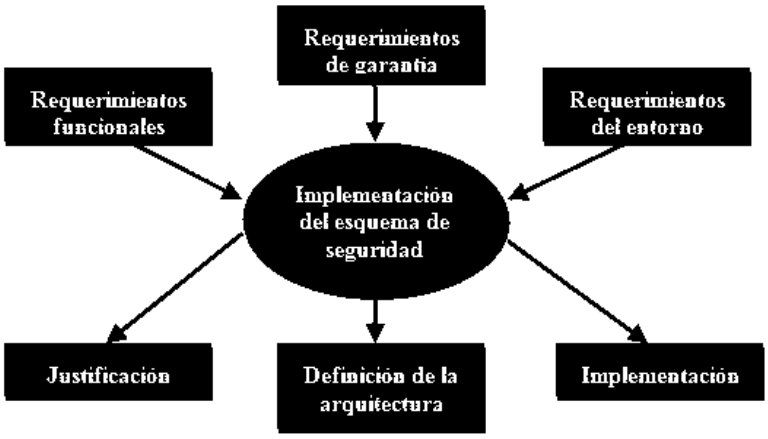


Figura 4.10 Implantación del esquema de seguridad

k) Implementación

En este proceso se llevan a cabo la instalación de las herramientas de seguridad, siendo las indicaciones dadas por el fabricante a través de los manuales y configurándolas de acuerdo con las políticas de seguridad, para lo cual:

- Se instalan las herramientas seleccionadas.
- La configuración de las herramientas se hace obedeciendo las políticas de seguridad.
- Se lleva a cabo las pruebas pertinentes.
- El esquema de seguridad está en reproducción.

4.4 Análisis de riesgos

Podemos definir el riesgo como: la posibilidad de que ocurra algún evento negativo para las personas y/o empresas. Ya que cualquier persona o entidad está expuesta a una serie de riesgos derivados de factores internos y externos, tan variables como su propio personal, su actividad, la situación económica, la asignación de sus recursos financieros o la tecnología utilizada. (Rodríguez, 1995)

Los equipos de cómputo que habitualmente se utilizan en las empresas están sujetos al riesgo de que ocurra alguna eventualidad que los dañe y debido a que no existe una seguridad total y las medidas de seguridad no pueden asegurar al 100% la protección en contra de las vulnerabilidades, es imprescindible realizar periódicamente en una organización, un análisis de riesgos, para identificar las consecuencia probables o los riesgos asociados con las vulnerabilidades, y así, lograr un manejo de riesgo tras la implementación y mantenimiento de controles que reduzcan los efectos de éste a un nivel aceptable.

El análisis de riegos proporciona herramientas útiles para cuantificar el riesgo y evaluar si este análisis es adecuado, tomar medidas para reducirlo, además intenta mantener un balance económico entre el impacto de los riesgos y el costo de las soluciones de un programa efectivo de seguridad destinadas a manejarlos.

En un proceso de análisis del riesgo debe considerarse la siguiente terminología (López Barrientos & Quezada Reyes, 2006):

1. *Activo:* es todo aquello con valor para una organización y que necesita protección – datos infraestructura, hardware, software, personal y su experiencia, información, servicios-.
2. *Riesgo:* posibilidad de sufrir algún daño o pérdida.
3. *Aceptación del riesgo:* decisión para aceptar un riesgo.
4. *Análisis de riesgo:* uso sistemático de información disponible para identificar las fuentes y para estimar qué tan seguido determinados eventos no deseados pueden

ocurrir y la magnitud de sus consecuencias. Uso sistemático de la información para describir y calcular el riesgo (tabla 4.1). Evaluación de amenazas y vulnerabilidades de la información y su impacto (ver tabla 4.2) en el procesamiento de la información así como su frecuencia de ocurrencia (ver tabla 4.3).

Tabla 4.1. Un ejemplo de la escala del riesgo (López Barrientos & Quezada Reyes, 2006) pág. 156

Cálculo del riesgo de incidencia por año	Clasificación
0	Ninguna
1 – 3	Baja
4 – 7	Media
8 – 14	Alta
15 – 19	Crítica
20 – 30	Extrema

Tabla 4.2. Un ejemplo de impacto del acontecimiento (López Barrientos & Quezada Reyes, 2006) pág. 156

Daño del acontecimiento	Grado del daño	Clasificación
Insignificante	Sin impacto	0
Menor	No se requiere un esfuerzo extra para reparar	1
Significante	Daño tangible, esfuerzo extra requerido para reparar	2
Dañino	Gasto significante requerido de recursos. Daño a la reputación y a la confianza	3
Serio	Pérdida de la conexión Compromiso de grandes cantidades de datos o servicios	4
Grave	Apagado permanente Compromiso total	5

Tabla 4.3. Un ejemplo de la frecuencia de ocurrencia de un acontecimiento (López Barrientos & Quezada Reyes, 2006) pág. 156

Acontecimiento	Frecuencia	Clasificación
Insignificante	Sin prioridad de que ocurra	0
Muy bajo	2 – 3 veces cada 5 años	1
Bajo	< = una vez por año	2
Medio	< = una vez cada 6 meses	3

Alto	< = una vez por mes	4
Muy alto	= > una vez por mes	5
Grave	= > una vez por día	6

5. *Manejo de riesgo:* proceso de identificación, control y minimización o eliminación de riesgos de seguridad que pueden afectar sistemas de información, por un costo aceptable.

6. *Evaluación del riesgo:* comparación de los resultados de un análisis del riesgo con los criterios estándares del riesgo u otros criterios de decisión.

7. *Impacto:* pérdidas como resultado de la actividad de una amenaza, las pérdidas son normalmente expresadas en una o más áreas de impacto –destrucción, denegación de servicios, revelación o modificación-.

8. *Pérdida esperada:* el impacto anticipado y negativo a los activos debido a una manifestación de la amenaza.

9. *Vulnerabilidad:* una condición de debilidad.

10. *Amenaza:* una acción potencial (que puede suceder o existir, pero no existe aún) con la posibilidad de causar daño.

11. *Riesgo residual:* el nivel de riesgo que queda después de la consideración de todas las medidas necesarias, los niveles de vulnerabilidad y las amenazas relacionadas. Éste debe ser aceptado como es o reducirse a un punto donde pueda ser aceptado.

12. *Control:* son los protocolos y mecanismos de protección que permiten el cumplimiento de las políticas de seguridad de la organización.

Un análisis de riesgo de seguridad es un procedimiento para estimar el riesgo de los activos de cómputo relacionados y la pérdida debido a la manifestación de las amenazas. El procedimiento primer determina el nivel de vulnerabilidad del activo tras identificar y evaluar el efecto de los controles colocados en el lugar. Un nivel de vulnerabilidad de activo para cierta amenaza se determina con controles que se encuentran en el lugar en el momento en el que se realiza el análisis del riesgo.

Un análisis de riesgos de seguridad define el ambiente actual y realiza acciones correctivas recomendadas si el riesgo residual no es aceptable; es un parte virtual de cualquier programa de manejo de riesgo de seguridad. El proceso de análisis de riesgo debe ser realizado con suficiente regularidad para asegurar que cada aproximación del manejo del riesgo de la organización sea respuesta real a los riesgos actuales asociados con la información de sus activos. El manejo de riesgos debe decir si acepta el riesgo residual o implementa las actividades recomendadas.

Las relaciones entre los elementos de un análisis del riesgo se muestran en la figura 4.11.

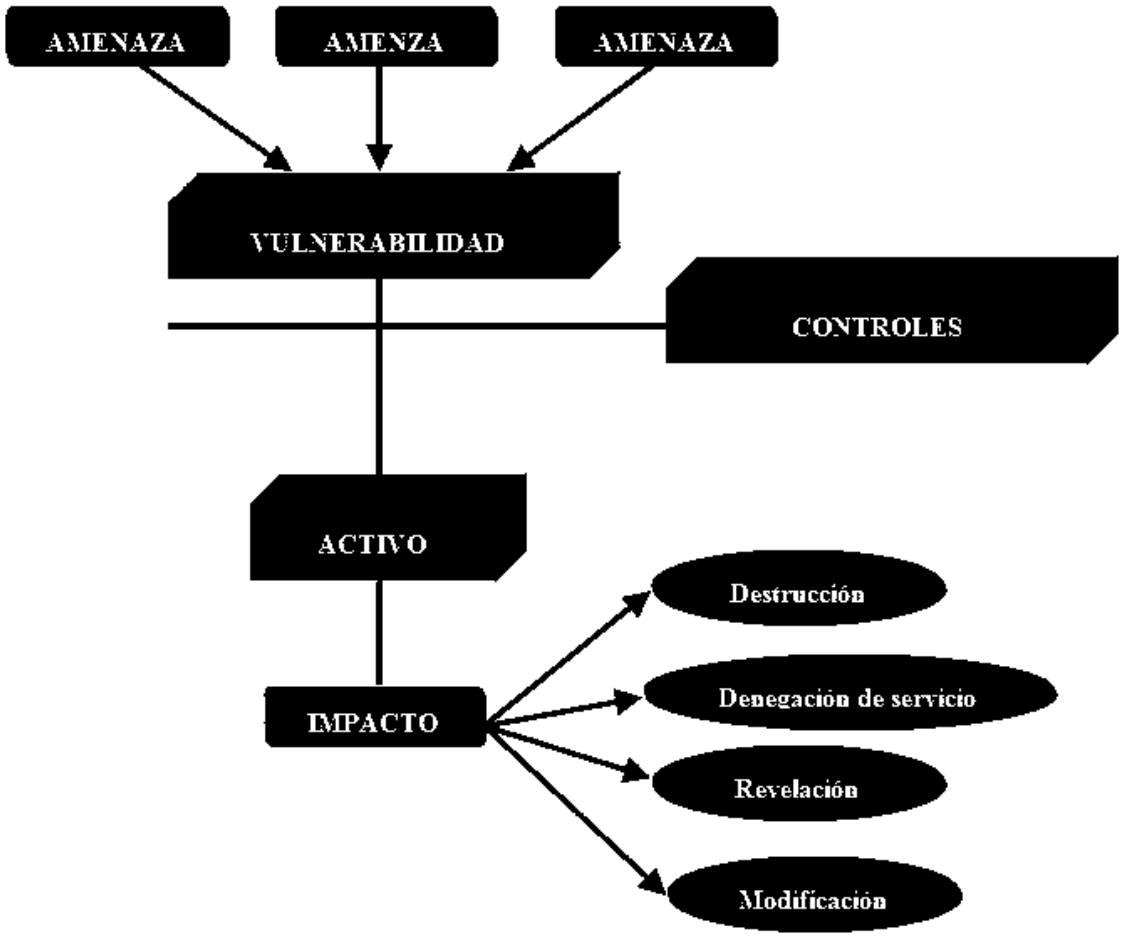


Figura 4.11 Relaciones entre los elementos de un análisis de riesgo

El objetivo del análisis de riegos es tener capacidad de:

- Identif**i**car, evaluar y manejar los riesgos de seguridad.
- Estimar la exposición de un recurso a una amenaza determinada.
- Determinar qué combinación de medidas de seguridad proporcionará un nivel de seguridad razonable a un costo aceptable.
- Tomar mejores decisiones en seguida de la información.
- Enfocar recursos y esfuerzos en la protección de activos

4.4.1 Tipos de análisis del riesgo

Una de las principales funciones del análisis del riesgo de seguridad es poner este proceso sobre una base más objetiva.

Existen dos tipos esenciales del análisis del riesgo.

1. Análisis cuantitativo del riesgo

Todos los activos, sus recursos y los controles se identifican, y se evalúan en términos monetarios. Todas las amenazas potenciales se identifican y se estima la frecuencia de su ocurrencia, estas amenazas se comparan con las vulnerabilidades potenciales del sistema de tal forma que se identifiquen las áreas que son sensibles.

Posteriormente el análisis cuantitativo del riesgo hace uso del término Expectativa de Pérdida Anual (ALE) o Costo Anual Estimado (EAC), el cual es calculado para cierto acontecimiento simplemente multiplicando la frecuencia de la ocurrencia de la amenaza por el valor del activo o clasificación del daño. Para esto, es necesario recolectar con detalle estimaciones exactas utilizando técnicas matemáticas y estadísticas.

De esta forma se puede decidir si los controles existentes son adecuados o si se requiere la implementación de otros, esto se observa cuando el producto obtenido tras multiplicar el valor del activo por la frecuencia de la ocurrencia de la amenaza en un período de tiempo determinado por la duración del control es menor que el costo de dicho control.

Los problemas con este tipo de análisis de riesgo se asocian generalmente a la falta de fiabilidad y a la inexactitud de los datos y algunas veces puede interpretarse erróneamente los resultados.

2. Análisis cualitativo del riesgo

En lugar de establecer valores exactos sedan notaciones como alto, bajo, medio que representan la frecuencia de ocurrencia y el valor de los activos. La desventaja es que pueden existir áreas significativamente expuestas que no hayan sido identificadas como posibles fuentes de riesgo.

Ambos tipos de análisis del riesgo hacen uso de los siguientes elementos interrelacionados:

a) Amenazas: las amenazas están siempre presentes en cada sistema.

b) Vulnerabilidades: las vulnerabilidades permiten que un sistema sea más propenso a ser atacado por una amenaza o que un ataque tenga mayor probabilidad de tener éxito o impacto.

c) Controles: son las medidas contra las vulnerabilidades. Existen cuatro tipos:

   - Los controles disuasivos reducen la probabilidad de un ataque deliberado.

- Los controles preventivos protegen vulnerabilidades y hacen que un ataque fracase o reduzca su impacto.
- Los controles correctivos reduce el efecto de un taque.
- Los controles detectores descubren ataques y disparan controles preventivos o correctivos.

Estos tres elementos pueden ser ilustrados mediante un modelo relacional simple que se aprecia en la figura 4.12.

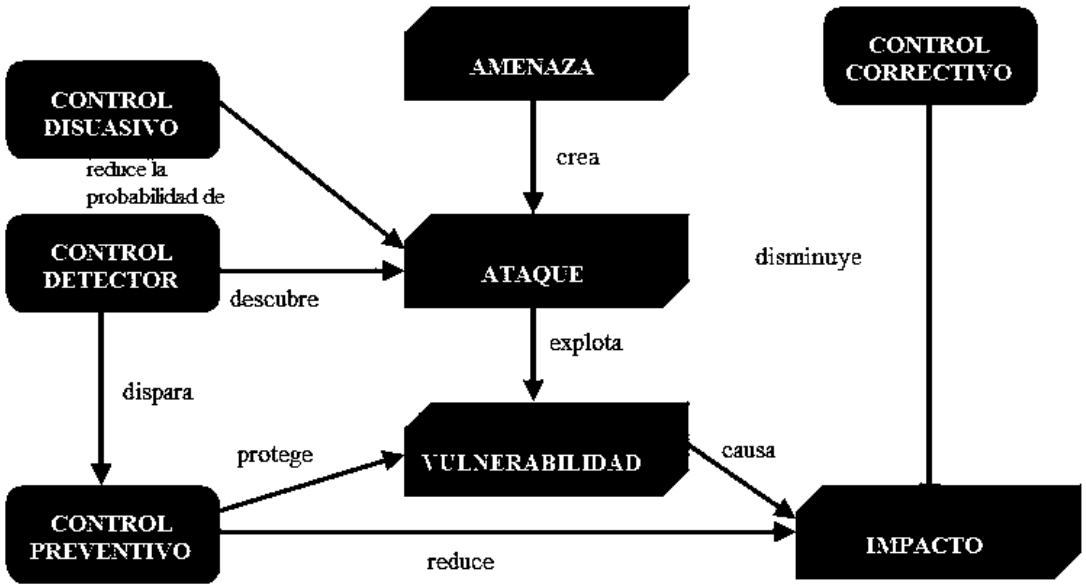


Figura 4.12 Modelo relacional simple

4.4.2 Cómo establecer los requerimientos y riesgos de seguridad

Existen tres fuentes principales que deben considerarse para que una organización identifique sus requerimientos de seguridad:

1. La primera fuente se deriva de determinar los riesgos de la organización. A través de la evaluación del riesgo se identifican las amenazas a los activos y la vulnerabilidad de éstos, también se evalúa la probabilidad de ocurrencia y se estima el potencial de impacto.

2. La segunda fuente se refiere a los requerimientos legales, regulatorios, contractuales y establecidos que una organización, sus socios comerciales y proveedores de servicio tienen que satisfacer.

3. La tercera fuente es el conjunto particular de principios, objetivos y requerimientos para el procesamiento de la información que una organización ha desarrollado para mantener sus operaciones.

Los requerimientos de seguridad son identificados mediante una evaluación metódica de riesgos de seguridad. Las técnicas de evaluación de riesgo pueden ser aplicadas a toda la organización, o sólo en algunas partes, como en los sistemas individuales de información, componentes específicos del sistema o servicios donde esto es factible, realista y útil.

La evaluación del riesgo es una consideración sistemática de:

- El daño al negocio es probablemente debido a una falla de seguridad, tomando en cuenta las consecuencias potenciales de una pérdida de confidencialidad, integridad o disponibilidad de la información y otros activos.

- La probabilidad real de la ocurrencia de una falla ante amenazas y vulnerabilidades comunes y de controles recientemente implementados.

Los resultados de esta evaluación ayudarán a guiar y determinar la acción apropiada de administración y las prioridades para manejar los riesgos de seguridad de la información.

Es necesario realizar revisiones periódicas de riesgos de seguridad y controles implementados para:

- Tomar en cuenta los cambios de requerimientos de negociación y las prioridades.

- Considerar nuevas amenazas y vulnerabilidades.

- Confirmar que los controles son efectivos y apropiados.

Las evaluaciones de riesgo son generalmente verificadas primero en un nivel alto, como medio para establecer la prioridad de los recursos en áreas de alto riesgo, y posteriormente en un nivel más detallado para analizar los riesgos específicos.

4.4.3 Pasos del análisis del riesgo

Cualquier análisis del riesgo de seguridad debe indicar:

1 El actual nivel de riesgo.

2 Las consecuencias probables.

3 Qué hacer con el riesgo residual si es muy alto.

Los tres elementos principales en un análisis de riesgo son:

1. Un balance del impacto o del costo de alguna dificultad específica si ésta sucede.

2. Una medida de la efectividad de los controles dentro del lugar,

3. Una serie de recomendaciones para corregir o minimizar los problemas identificados.

El proceso de análisis de riesgo consiste de ocho pasos interrelacionados:

a) Identificar y evaluar los activos

Identificar y asignar un valor a los activos que necesitan protección. El valor del activo se basa en su costo, sensibilidad, misión crítica, o la combinación de estas propiedades.

b) Identificar las amenazas

Después de identificar los activos que requieren protección, las amenazas a éstos deben ser identificadas y examinadas para determinar cuál sería la pérdida si dichas amenazas se presentan.

c) Identificar/describir vulnerabilidades

El nivel de riesgo se determina analizando la relación entre las amenazas y las vulnerabilidades. Un riesgo existe cuando una amenaza tiene una vulnerabilidad correspondiente, aunque hay áreas de alta vulnerabilidad que no tienen consecuencia si no presentan amenazas.

d) Determinar el impacto de la ocurrencia de una amenaza

Cuando la explotación de una amenaza ocurre, los activos sufren cierto impacto. Las pérdidas son catalogadas en áreas de impacto llamadas:

- Revelación: cuando la información es procesada y se pierde la confidencialidad.

- Modificación: el efecto de la manifestación de una amenaza cambia de estado original del activo

- Destrucción: el activo es logrando su completa pérdida.
- Denegación de servicio: pérdida temporal de los servicios.

e) Controles en el lugar

La identificación de los controles es parte del proceso de recolección de datos en cualquier proceso de análisis del riesgo. Existen dos tipos principales:

- Controles requeridos: todos los controles de es esta categoría pueden ser definidos con base en una o más reglas escritas.
- Controles discrecionales: este tipo de controles es elegido por los administradores.

f) Determinar los riesgos residuales (conclusiones)

Siempre existirá un riesgo residual por lo tanto, debe determinarse cuándo el riesgo residual, es aceptable o no. El riesgo residual toma la forma de las conclusiones alcanzadas en el proceso de evaluación. Las conclusiones deben identificar:

- Las tareas que tienen alta vulnerabilidad junto con la probabilidad de ocurrencia de la amenaza.
- Todos los controles que no están dentro del lugar.

g) Identificar los controles adicionales (recomendaciones)

El siguiente paso es identificar la forma más efectiva y menos costosa para reducir el riesgo a un nivel aceptable. Un intercambio operacional – el cual puede tomar la forma de costo, convivencia, tiempo, o una mezcla de los anteriores- debe realizarse al mismo tiempo que los controles adicionales son implementados. Las recomendaciones son:

- Recomendación de controles requeridos: controles requeridos u obligatorios que no se encuentran en el lugar son las primeras recomendaciones.
- Recomendaciones de controles discrecionales: la segunda recomendación generalmente identifica los controles direccionales necesarios para reducir el nivel de riesgo.

h) Preparar un informe del análisis del riesgo

El proceso de análisis del riesgo determina si los controles son efectivos. Cuando el análisis está completo, un informe de la evaluación del riesgo debe prepararse. Los detalles técnicos del reporte deben incluir como mínimo:

- Niveles de vulnerabilidad.
- Amenazas correspondientes y su frecuencia.
- El ambiente usado.
- Conexión del sistema
- Nivel o niveles de sensibilidad de los datos
- Riesgo residual, expresado en una base individual de vulnerabilidad.
- Cálculos detallados de la expectativa de pérdida anual.

Es esencial asegurarse que los controles y el gasto que implica sean completamente proporcionales a los riesgos a los cuales se expone la organización.

4.4.4 Consideraciones adicionales durante el análisis del riesgo.

En cualquier análisis del riesgo deben tomarse en cuenta tres costos o valores fundamentales:

1. *Costo del sistema informático (Cr):* valor de los recursos y la información a proteger.
2. *Costo de los medios necesarios (Ca):* qué medios y el costo respectivo que un criptoanalista requiere para romper las medidas de seguridad establecidas en el sistema.
3. *Costo de las medidas de seguridad necesarias (Cs):* medidas y su costo para salvaguardar los bienes informáticos.

Para que la política se seguridad del sistema sea lógica debe cumplirse la siguiente relación:

$$Ca > Cr > Cs$$

En el que Ca > Cr, significa que el ataque al sistema debe ser más costoso que su valor.

El que Cr > Cs, significa que no debe costar más la información que la información protegida. Si esto ocurre, resultaría conveniente no proteger el sistema y volver a obtener la información en caso de pérdida.

a) Análisis del valor del sistema informático

Al evaluarse el sistema informático que se desea proteger, su valor puede desglosarse en dos parte fundamentales:

- El valor intrínseco del producto que se va a proteger.
- Los costos derivados de su pérdida.

b) Valor intrínseco

Es la parte más sencilla de valorar, puesto que en la mayoría de los casos se pueden establecer valores objetivos y medibles de los recursos e información. Se trata de enumerar los recursos incluidos en el sistema informático y de establecer su valor.

c) Costos derivados

Dependiendo del tipo de sistema con que se trata, pueden ser muy distintos, o su valor e importancia relativa pueden variar enormemente. En términos generales se puede incluir los siguientes conceptos:

- Valor de sustituir el hardware.
- Valor de sustituir el software.
- Valor de los resultados.
- Costo de reproducir los experimentos significativos.
- Costo de regenerar la información personal.

CAPÍTULO 5

Aspectos Legales y Éticos

En este capítulo se mencionan los principales asuntos que deben ser legislados dentro de las leyes Mexicanas en materia de leyes informáticas, como son los delitos informáticos, contratos electrónicos y firma electrónica, la propiedad intelectual, cómputo forense, entre otros, y así poder regular la conducta del hombre en la sociedad, además de proporcional algunos códigos de ética que apoyen al comportamiento moral del hombre.

CAPÍTULO 5

Aspectos Legales y Éticos

5.1 Leyes Mexicanas.

El Derecho surge como un medio efectivo para regular la conducta del hombre en sociedad, regula la conducta y los fenómenos sociales a través de leyes; cabe señalar que el proceso de creación de las leyes es largo y lento, por esto presenta un grave rezago considerable en materia de leyes informáticas.

Los principales asuntos que se deberían legislar son:

- Delitos informáticos.
- Contratos electrónicos y firma electrónica.
- Protección de la privacidad y de la información.
- Propiedad Intelectual.
- Cómputo forense.
- Contenidos en Internet.
- Comercio electrónico.
- Aspectos laborales.

5.1.1 Delitos informáticos.

El delito informático puede considerarse como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena. También los delitos informáticos se definen como "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".

Encontramos sancionadas las siguientes conductas:

- Modificación, destrucción o provocar la pérdida de información contenida en sistemas o equipos informáticos, (virus, gusanos)

- Conocer o copiar la información contenida en sistemas o equipos.

  Es importante señalar que las penas varían si se trata de sistemas o equipos de particulares, del Estado o de las Instituciones que integran el Sistema Financiero, asimismo se agravan si tratándose de sistemas o equipos del Estado, el presunto

contaba con autorización para el acceso. Las penas se incrementan si son realizadas por empleados del Sistema Financiero o si se obtiene provecho de la información obtenida (en éste caso, estaríamos en presencia de fraude, si bien el Código no lo tipifica como tal). Sin embargo, inexplicablemente no se sancionan las conductas descritas tratándose de equipos o sistemas privados cuando el agente cuenta con autorización para el acceso.

- Uso y/o reproducción no autorizada de programas informáticos con fines de lucro (piratería).

  En este caso vale la pena resaltar que es ésta una de las conductas antijurídicas en esta materia mejor regulada, en virtud de la armonización lograda con la Ley Federal del Derecho de Autor, misma que protege los programas de cómputo. También cabe aclarar que se sanciona asimismo al que fabrique, importe, venda o arriende algún sistema o dispositivo destinado a descifrar señales cifradas de satélite que contengan programas o algún dispositivo o sistema diseñado para desactivar la protección de un programa de cómputo. Las penas por la reproducción de obras protegidas con fines de lucro son fuertes (2 a 10 años de prisión y de 2000 a 20,000 días de multa).

- Ataque a las vías de comunicación y obtención de información que pasa por el medio.

  El Código Penal Federal sanciona con uno a cinco años de prisión y 100 a 10,000 días de multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas, o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, video o datos.

  Aquí encuadran, entre otras, las conductas encaminadas a obtener información financiera o de crédito de las personas (al hacer una compra por Internet, por ejemplo), así como el interceptar correos electrónicos antes de que lleguen a su destinatario; sin embargo, no se tipificaría el hecho de acceder al buzón de correo electrónico de alguien y leer su correspondencia, lo cual crea un vacío legal al resultar controversial (o al menos, merecer interpretación) el poder encuadrar esta conducta en el delito de violación de correspondencia, que se refiere "al que abra o intercepte una comunicación escrita que no esté dirigida a él".

- Pornografía infantil.

  En este caso la ley específicamente hace alusión al caso de la exhibición corporal, lasciva o sexual de menores de 18 años mediante anuncios electrónicos, sancionando al que procura, facilita, induce u obliga a los menores, así como al o los que elaboran, reproducen, venden, arriendan, exponen, publicitan o transmiten el material referido. Éstas conductas se punen con prisión que va de los 5 a los 14 años y multa de 1000 a 3000 días, pero a quien dirija asociación delictuosa dedicada a los fines descritos, se le impondrán de 8 a 16 años y de 3,000 a 10,000 días de multa.

- Asociación delictuosa y pandilla.

  El Código Penal sanciona el hecho de formar parte de alguna asociación o banda con el propósito de delinquir y también regula de forma especial a las pandillas, entendiendo por éstas la reunión habitual, ocasional o transitoria de tres o más personas que sin estar organizadas con fines delictivos, llegan a cometer algún delito.

  A este respecto también cabe la consideración de si encuadrarían en la descripción del tipo penal las asociaciones, bandas y pandillas electrónicas, es decir, gente que sin conocerse siquiera, se reúne electrónicamente a través de Internet para planear la comisión de ilícitos, o bien, que reuniéndose con otros fines, llegan a intervenir en la realización de algún delito, sean éstas habituales, ocasionales o de primera vez.

5.1.2 Contratos electrónicos y firma electrónica.

La firma electrónica es un conjunto de datos adjuntados o asociados a un mensaje y utilizados como medio para identificar al autor y garantizar la integridad de los documentos digitales. Entonces, es el resultado de obtener un patrón que se asocie biunívocamente a un individuo y su voluntad de firmar, utilizando determinados mecanismos, técnicas o dispositivos electrónicos que garanticen que después no pueda negar su autoría.

El fin de la firma digital es el mismo que el de la firma autógrafa: Prestar conformidad y responsabilizarse con el documento firmado. No obstante de los conceptos que anteceden se desprende que hay distintos niveles de "confiabilidad" y/o de "seguridad" de la firma electrónica.

Al hablar de contratos nos referimos al acuerdo de voluntades en orden a una determinada convención destinada a reglar sus derechos. Se fundamenta principalmente en la autonomía de la voluntad de las partes. Pero en el mundo de Internet, las nuevas estrategias de contratación y los contratos electrónicos no son más que un acuerdo de voluntades, aunadas a través de redes digitales, destinadas a crear, modificar o transferir derechos de las partes.

Ésta materia se encuentra regulada en varias leyes:

a) La Ley de Instituciones de Crédito

Autoriza a las mismas a "pactar la celebración de sus operaciones y la prestación de servicios con el público, mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos...". La propia ley determina asimismo, que en los contratos respectivos deben de establecerse cuáles serán los medios para identificar al usuario y para hacer constar la creación, transmisión, modificación o extinción de los derechos y obligaciones inherentes a las operaciones de que se trate, otorgándoles validez y valor probatorio a los medios de identificación que se establezcan en sustitución de la firma autógrafa.

b) La Ley del Mercado de Valores

Al regular el contrato de intermediación bursátil, autoriza a las partes a convenir libremente el uso de télex, telefax o cualquier otro medio electrónico, de cómputo o telecomunicaciones para el envío, intercambio o confirmación de las órdenes de la clientela inversionista, debiendo las partes precisar las claves de identificación recíproca y las responsabilidades que conlleve su utilización.

c) El Código de Comercio

La primera vez que se legisló en materia de comercio electrónico en México fue en mayo de 2000, con las primeras reformas realizadas al Código de Comercio, al Código Civil que después sería federal y al Código Federal de Procedimientos Civiles; posteriormente, en agosto de 2003, se volvió a reformar el Código de Comercio, incorporando un Título Segundo referente al Comercio electrónico. Básicamente, se autoriza el empleo de medios electrónicos, ópticos y de cualquier otra tecnología en los actos de comercio y la formación de los mismos, sentando las bases de lo que se entiende por mensaje de datos y firma electrónica,

estableciendo la necesidad de que se confirme el vínculo entre un firmante y los datos de creación de la firma electrónica mediante un certificado, que deberá ser expedido por un prestador de servicios de certificación autorizado en este caso por la Secretaría de Economía. El Código dicta los lineamientos para determinar cuándo y dónde se presume que un mensaje de datos ha sido enviado y recibido, las formalidades a seguir cuando el acto deba constar por escrito o ante fedatario público, los requisitos para que una firma electrónica se considere fiable, las obligaciones del firmante y del destinatario, los requisitos para ser prestador del servicio de certificación, las obligaciones de los prestadores de este servicio y los elementos de un certificado (nacional o extranjero) válido.

d) La Ley Federal de Protección al Consumidor

Protege como confidencial la información que éste proporcione al proveedor, prohibiendo su difusión a otros proveedores ajenos, salvo autorización expresa e imponiendo al proveedor la obligación de utilizar los elementos técnicos disponibles para brindar confidencialidad y seguridad a la información proporcionada. También obliga al proveedor a entregar al consumidor antes de la transacción, sus números telefónicos y domicilio físico en donde pueda presentar reclamaciones.

e) El Código Civil Federal

Al regular el consentimiento, menciona que "será expreso cuando se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos..."; asimismo, equipara a la oferta hecha entre presentes la realizada por medios electrónicos, ópticos o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.

5.1.3 Protección de la privacidad y de la información.

La intimidad o Privacidad podemos definirla como: "Conjunto de circunstancias, cosas, experiencias, sentimientos y conductas que un ser humano desea mantener reservado para sí mismo, con libertad de decidir a quién le da acceso. Que impone a todos los demás la obligación de respetar". En Internet podemos entender esto como el derecho de una persona a no ser publicitada, exhibida.

Ésta materia se encuentra regulada en varias leyes:

I. La Ley Federal de Protección al Consumidor

Como veíamos en el punto anterior, protege como confidencial la información que éste proporcione al proveedor, prohibiendo su difusión a otros proveedores ajenos, salvo autorización expresa e imponiendo al proveedor la obligación de utilizar los elementos técnicos disponibles para brindar confidencialidad y seguridad a la información proporcionada.

II. La Ley Federal del Derecho de Autor

Al proteger las bases de datos que por razones de disposición de su contenido constituyan obras intelectuales, establece que la información privada de las personas contenidas en dichas bases no podrá ser divulgada, transmitida ni reproducida, salvo con el consentimiento de la persona de que se trate.

III. La Ley de Instituciones de Crédito

Sanciona con prisión y multa al que "obtenga o use indebidamente la información sobre clientes u operaciones del sistema bancario sin contar con las autorización correspondiente…"; sin embargo, sólo puede imponer pena de prisión un juez penal y su fundamento tiene por fuerza que ser una ley penal. El Código Penal Federal sanciona al que indebidamente utilice información confidencial reservada a la institución o a persona facultada, con el objeto de producir, alterar o enajenar tarjetas o documentos utilizados para el pago de bienes o servicios o para disposición de efectivo, por lo que como se ve, la disposición no va encaminada a proteger la privacidad, sino sólo en la medida en que se evita el fraude.

IV. Existe una iniciativa de Ley Federal de Protección de Datos Personales

La ley define lo que se entiende por datos personales, datos sensibles, banco de datos, tratamiento de datos, usuario, responsable e interesado y establece que toda persona tiene derecho a ser informada sobre la existencia de un archivo de datos sobre ella, la identidad y domicilio del responsable del mismo y su posibilidad de ejercer derechos de acceso, complementación, rectificación, reserva y cancelación. Se determinan los derechos y obligaciones de los responsables de archivos o bases de datos, así como la creación de un Instituto encargado de controlar, organizar, estructurar, y vigilar la protección de datos

personales. También se crea la acción de protección de datos personales, como procedimiento civil.

V. Por lo que se refiere al spam,

Desde finales de 2003, la PROFECO colaboró activamente con países miembros del comité de políticas de consumidor para la elaboración de un documento titulado: Background Paper on Spam en donde se hace un análisis del problema de spam y trata de esbozar las herramientas legales que posee cada una de las agencias con la finalidad de combatir esta práctica.

Posteriormente como resultado de las reformas a la Ley Federal de Protección al Consumidor del 4 de Febrero de 2004, la PROFECO reforzó y mejoró el marco jurídico en los siguientes rubros:

a. Las prácticas de mercadotecnia y de publicidad con el objeto de proteger al consumidor mexicano de los mensajes no solicitados que constantemente envían empresas de telemercadeo y publicidad por correo electrónico.
b. Veracidad de la información sobre bienes y servicios para evitar prácticas abusivas o engañosas por parte de empresas y proveedores.
c. Celebración de contratos de adhesión por vía electrónica y servicios adicionales o conexos no previstos en el contrato original.
d. La presentación de denuncias por vía electrónica por incumplimiento a las disposiciones de la LFPC, la Ley Federal de Metrología y Normalización, normas oficiales mexicanas y demás disposiciones aplicables.

5.1.4 Propiedad Intelectual.

La propiedad intelectual supone el reconocimiento de un derecho de propiedad especial en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano.

En México, están protegidos los programas de cómputo así como las bases de datos que por su composición constituyan obra intelectual, como apuntamos anteriormente. La ley que tutela éstos derechos es la Ley Federal del Derecho de Autor, misma que entiende por programa de cómputo "la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica".

La Ley protege programas tanto operativos como aplicativos y deja fuera a los que tienen por objeto causar efectos nocivos. Autoriza al usuario legítimo a hacer las copias que le permita la licencia, o bien, una sola que sea indispensable para la utilización del programa o sea destinada sólo para resguardo. El autor tiene derecho de prohibir además de la reproducción, la traducción, adaptación o arreglo al programa, así como su distribución o descompilación. Se prohíbe además la importación, fabricación, distribución y utilización de aparatos o prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo. La violación a lo anterior, constituye una infracción en materia de comercio, sancionada con multa por el Instituto Mexicano de la Propiedad Intelectual. Además, está la tipificación penal a que aludimos en el punto uno de este trabajo.

En México existe el reconocimiento que hace el Estado a través de la Ley Federal del Derecho de Autor (LFDA) a favor de todo creador de programas de cómputo otorgando protección para que el autor goce de prerrogativas y privilegios exclusivos de carácter personal y patrimonial.

La protección que otorga esta ley se concede a los programas de cómputo desde el momento en que hayan sido fijados en un soporte material, por lo que no se requiere ni registro ni documento de ninguna especie, sin embargo para efectos legales es recomendable que se realice el registro en el Instituto Nacional del Derecho de Autor (INDAUTOR) quien garantiza el reconocimiento de este derecho a través de un antecedente fechado por esta institución de carácter oficial, quien ayudara a resolver controversias en caso de suscitarse.

Para el registro de programas de cómputo en el INDAUTOR se tienen que cumplir los siguientes requisitos:

Se deben presentar por duplicado, engargolados o en forma tal que se evite su maltrato o pérdida:

- Síntesis de la función del programa de cómputo
- Relación ascendente de archivos que componen el programa
- Las diez primeras hojas y las diez ultimas hojas del código fuente.
- Ejemplar del programa de cómputo completo grabado en cualquier soporte material.

Los documentos necesarios se pueden descargar de:

http://www.sep.gob.mx/wb/sep1/sep1_Formatos_y_requisitos_para_tramites

Que son:

- Solicitud de registro del programa de cómputo RPFA-01 debidamente llenado.
- RDPA-01 A1, Hoja adjunta para los casos en que haya varios autores y titulares.
- RDPA-01 A2, Hoja adjunta para los casos en que se hace referencia a las diversas obras primigenias que se utilizaron para la creación de una obra derivada.
- Formato SHCP-5 Original de la forma en la que conste el pago de los derechos correspondientes.
- En caso de haberlo, carta poder para el gestor o representante legal.
- Si el solicitante no es el titular de los derechos patrimoniales de autor (Facultad que posee el autor de explotar su obra con fines de lucro), deberá acreditar su titularidad con el original de la carta de colaboración, contrato o documento respectivo.
- Si el titular de los derechos patrimoniales de autor es una persona moral, deberá acreditar su personalidad y la de su representante.

5.1.5 Cómputo forense.

Es el proceso de aplicación de técnicas científicas y analíticas a infraestructura de cómputo, para identificar, preservar, analizar y presentar evidencia de manera que sea aceptable en un procedimiento legal.· El término "forense" proviene de foro -sitio donde los tribunales juzgan las causas- implica un ejercicio y aplicación de índole técnica y de procedimientos mediante los cuales se aprovechan una o varias ramas de la investigación criminal o de ciencias conexas que estudian y resuelven casos concretos ligados habitualmente a situaciones legales o jurídicas. Lo forense es también establecer premisas y fundar conclusiones específicas, amoldándolas para ello a un proceso, siguiendo un método estructurado de tal manera que permita formular una resolución expresada en términos técnicos.

Apenas legislada esta materia, diversos ordenamientos legales se limitan a otorgarles valor probatorio a los documentos o instrumentos que se obtengan por medios electrónicos (Código de Comercio, Ley de Instituciones de Crédito, Ley del Mercado de Valores). El Código Federal de Procedimientos Civiles expresamente reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología, debiéndose estar a la fiabilidad del método con el que haya sido generada, comunicada, recibida o archivada y si es posible atribuir a las personas obligadas el contenido de la misma, siendo accesible para su siguiente consulta.

En este caso, además de la necesidad de unificar las diversas legislaciones del país tanto en materia penal como civil, se requiere ser más específicos ya que no se dice qué determina "la fiabilidad del método con el que haya sido generada…", por lo que es necesario remitir a estándares internacionales como son el ISO (International Standard Organization) y el IEEE (Institute of Electric and Electronic Engineers).

Pero además sería conveniente establecer ciertas obligaciones para los proveedores del servicio de Internet, y para los titulares de nombres de dominio, como el establecer cuentas abuse (para recibir quejas de los usuarios), llevar de manera organizada logs o bitácoras y tener identificables los números de teléfono, IP asignada y tiempo de conexión de los usuarios, para que sea más fácil en determinado momento para un perito en cómputo, reunir los documentos que deban aceptarse como prueba en un juicio.

5.1.6 Contenidos en Internet.

Es éste un asunto de los más difíciles en cuanto a regulación se trata, en virtud del carácter absolutamente internacional del Internet y de la enorme cantidad de sitios que existen. Se han hecho algunos esfuerzos por regular un adecuado uso de Internet, aislados y sin fructificar (Europa, Estados unidos de América). Este complejo asunto se manifiesta por ejemplo, en el hecho de que estando prohibidos los casinos en México, no exista forma alguna de evitar que las personas jueguen en casinos virtuales y mucho menos, de sancionarlas.

Consideramos que el único contenido de Internet que está prohibido y sancionado en nuestro país es el de la pornografía infantil, mencionado en un punto de este escrito.

En este aspecto vuelve a resaltar la necesidad de establecer obligaciones para los titulares de nombres de dominio, llevando une estricto registro de los mismos, así como para los proveedores del servicio.

5.2 Principales Tipos de Leyes.

Al estar constituido nuestro país como una República representativa, democrática, federal, en la que los Estados que la integran son libres y soberanos en cuanto a su régimen interior, si bien unidos por el pacto federal, encontramos que en la actualidad, los asuntos informáticos que inciden en el ámbito del Derecho Civil o Penal, pueden ser regulados por cada una de las Entidades Federativas a su libre y mejor parecer.

El Congreso Federal, constitucionalmente, tiene facultades exclusivas para legislar sobre: hidrocarburos, minería, industria cinematográfica, comercio, juegos con apuestas y sorteos, intermediación y servicios financieros, energía eléctrica y nuclear, derecho marítimo, ciudadanía, migración, vías generales de comunicación, correos, aguas, moneda, delitos federales, coordinación en materia de seguridad pública, fiscalización superior de la federación, leyes del trabajo reglamentarias del artículo 123 Constitucional, nacionalidad y extranjería, migración, salubridad , coordinación de la educación, generación, difusión y aplicación de conocimientos científicos y tecnológicos, entre otras.

De lo anterior podemos observar que todo el comercio electrónico, contratos electrónicos mercantiles, fenómenos informáticos que afecten vías generales de comunicación, delitos informáticos regulados por el Código Penal Federal (piratería, destrucción de información), los contenidos de Internet que impliquen delito federal (pornografía, casinos), el correo electrónico (si legalmente se equiparara al correo convencional) constituyen materia federal y por tanto, son o deberán ser regulados por leyes federales.

Sin embargo, los Estados pueden regular, en el ámbito de su competencia, las materias que no están expresamente reservadas a la Federación; por lo que en esta esfera entrarían los contratos civiles electrónicos, los delitos informáticos que incidan en el orden común, la admisión de documentos o medios electrónicos como prueba en los procesos penales o civiles, la protección a bases de datos privadas y todo aquel asunto que no toque materia federal.

En nuestra opinión, dada la importancia, la trascendencia, el carácter global e internacional de Internet, de las Tecnologías de Información y Comunicación y de las herramientas tecnológicas que pueden afectar las relaciones económicas y sociales, lo ideal u óptimo es que se eleve a nivel federal la materia informática.

A grandes rasgos, hemos descrito el panorama general del marco jurídico en materia informática en México, y podemos concluir que hasta el día de hoy, hemos avanzado en ciertas materias, así como hay otras en las que falta aún mucho camino, por lo que hemos señalado lo que consideramos más importante añadir o cambiar en nuestra legislación. Desde luego que se hace necesario un análisis minucioso, así como iniciativas específicas.

5.3 Ética.

La ética es la teoría del comportamiento moral de los hombres en sociedad, es decir, de cómo nosotros debemos vivir y en particular sobre cómo nosotros debemos vivir en relación con los demás. Para entender más afondo lo que es ética es necesario retomar las raíces de los vocablos moral y ética.

La palabra *moral* tiene su origen en el término del latín "*mos, moris*", cuyo significado es "costumbre". Conjunto de costumbres, creencias, valores y normas de una persona o grupo social determinado que orientan acerca del bien o del mal —o bien, correcto o incorrecto— de una acción.

Por otra parte, la palabra *ética* proviene del griego "Ethos" cuyo significado es "Carácter o modo de ser" en cuanto a la forma de vida también adquirida o conquistada por el hombre.

Por lo que la Ética en la Informática (EI) podría definirse las siguientes formas:

- Se define "como la disciplina que analiza los problemas éticos que son creados por las tecnologías computacionales 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.

- "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", esta definición está relacionada con los problemas conceptuales y los vacíos en las regulaciones que ha ocasionado la tecnología de la información.

- También se define a la EI "como la disciplina que identifica y analiza los impactos de las tecnologías de la información en los valores humanos y sociales", estos valores afectados son: la salud, la riqueza, el trabajo, la libertad, la democracia, el conocimiento, la privacidad, la seguridad o la autorrealización personal.

5.3.1 Objetivos

Para esta disciplina de EI se plantea varios objetivos:

- Descubrir y articular dilemas éticos clave en informática.

- 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.

- Utilizar la teoría ética para clarificar los dilemas éticos y detectar errores en el razonamiento ético.

- Proponer un marco conceptual adecuado para entender los dilemas éticos que origina la informática y además establecer una guía cuando no existe reglamentación de dar uso a Internet.

5.3.2 Deontología

Según el diccionario de la real academia de la lengua, es la ciencia o tratado de los deberes y normas morales. En un sentido más concreto, tiene que ver con el comportamiento moral o ético, es decir con los ***principios y normas morales que regulan las actividades humanas ante su relación con la sociedad.***

La deontología informática, por tanto trata, de la moral o ética profesional en el manejo del activo más importante que tenemos, un bien cada vez más apreciado, ***que es la información,*** a través de los códigos de ética.

"Los **códigos de ética** son sistemas de reglas establecidos con el propósito general de guiar el comportamiento de los integrantes de una organización y de aquellos con los cuales ésta actúa habitualmente: trabajadores, clientes, proveedores, contratistas, etc."

Los códigos de ética contienen principios claves, relacionados con el comportamiento y las decisiones tomadas de las diferentes profesiones que comprende el campo de la programación y la información, ya sean profesionales en ejercicio, educadores, gestores, directivos y responsables, así como educandos y estudiantes de la profesión.

Algunos códigos de ética son:

5.3.3 Código de ética del ingeniero mexicano[1]

El Ingeniero reconoce que el mayor mérito es el trabajo, por lo que ejercerá su profesión comprometido con el servicio de la sociedad mexicana, a tendiendo al bienestar y progreso de la mayoría.

Al transformar la naturaleza en beneficio de la humanidad, el Ingeniero debe acrecentar su conciencia de que el mundo es la morada del hombre y de que su interés por el universo es una garantía de la superación de su espíritu y del conocimiento de la realidad para hacerla más justa y feliz.

El Ingeniero debe rechazar los trabajos que tengan como fin atentar contra el interés general, de esta manera evitara situaciones que involucren peligro o constituyan una amenaza contra el medio ambiente, la vida, la salud y demás derechos del ser humano.

Es un deber ineludible del ingeniero sostener el prestigio de la profesión y velar por su cabal ejercicio; así mismo, mantener una actitud profesional amentada en la capacidad, la honradez, la fortaleza, la templanza, la modestia, la franqueza y la justicia, con la conciencia de subordinar el bienestar individual al bienestar social.

El Ingeniero debe procurar el perfeccionamiento constante de sus conocimientos, en particular de su profesión, divulgar su saber, compartir su experiencia, proveer

[1] Fuente: http://www.ingenieria.unam.mx/~guiaindustrial/valores/info/3/1.htm

oportunidades para la formación y capacitación de los trabajadores brindar reconocimiento, apoyo moral y material a la educación educativa donde realizo sus estudios de esta manera revertirá a la sociedad las oportunidades que ha recibido.

Es responsabilidad del Ingeniero que su trabajo se realice con eficiencia y apego a las disposiciones legales. En particular velara por el cumplimiento de las normas de protección a los trabajadores, establecidas en la legislación laboral mexicana.

En el ejercido de su profesión, el Ingeniero debe cumplir con diligencia los compromisos que haya asumido y desempeñara con dedicación y lealtad los trabajos que se le asignen, evitando anteponer sus intereses personales en la atención de los asuntos que se le encomienden, o coludirse para ejercer competencia desleal en perjuicio de quien reciba sus servicios.

Observara una conducta decorosa, tratando con respeto, diligencia, imparcialidad y rectitud, a las personas con las que tenga relación, particularmente a sus colaboradores, absteniéndose de incurrir en desviaciones o abuso de autoridad y de disponer o autorizar a un subordinado conductas ilícitas, así como de favorecer indebidamente a terceros.

Debe salvaguardar los intereses de la institución o personas para las que trabaje y hacer buen uso de los recursos que se le hayan asignado para el desempeño de sus labores.

Cumplirá con eficiencia que en ejercicio de sus atribuciones le dicten sus superiores jerárquicos, respetará y hará respetar su posición y trabajo; si discrepara de sus superiores tendrá la obligación de manifestar ante ellos las razones de su discrepancia.

El Ingeniero tendrá como norma crear y promover la tecnología nacional, pondrá especial cuidado en vigilar que la transformación tecnológica se adapte a nuestras condiciones conforme el marco legal establecido. Se obligara a guardar secreto profesional de los datos confidenciales que conozca en ejercido de su profesión salvo que sean requeridos por autoridades competentes.

5.3.4 Código de ética de la ACM (Association for Computing Machinery)

Este Código, consistente en 24 preceptos expresados como declaraciones de responsabilidad personal, identifica los elementos de tal compromiso.

Este código trata muchos de los aspectos, pero no todos, que los profesionales probablemente afrontarán. La Sección 1 perfila las consideraciones éticas fundamentales, mientras que la Sección 2 trata reflexiones adicionales, más específicas sobre la conducta profesional. Los preceptos de la Sección 3 incumben más específicamente a personas que tengan una función de liderazgo, bien sea en su lugar de trabajo o en calidad de voluntarias, como puede suceder en organizaciones tales como la ACM. Los principios que involucran conformidad con este Código se muestran en la Sección 4.

1. Preceptos Morales Generales

1.1 Contribuiré al bienestar de la sociedad y de la humanidad.
1.2 Evitaré daño a otros.
1.3 Seré honesto/a y confiable.
1.4 Seré justo/a y actuaré para no discriminar.
1.5 Respetaré los derechos de propiedad, incluyendo las patentes y derechos de autor.
1.6 Reconoceré adecuadamente la propiedad intelectual.
1.7 Respetaré la intimidad de otros.
1.8 Respetaré la confidencialidad.

2. Responsabilidades profesionales más específicas

2.1 Me esforzaré para alcanzar la mayor calidad, efectividad y dignidad en los procesos y productos del trabajo profesional.
2.2 Adquiriré y mantendré la capacitación profesional.
2.3 Conoceré y respetaré las leyes existentes relacionadas con el trabajo profesional.
2.4 Aceptaré y proporcionaré la adecuada revisión profesional.
2.5 Proporcionaré evaluaciones completas y extensas de los sistemas informáticos y sus consecuencias, incluyendo el análisis de los posibles riesgos.
2.6 Respetaré los contratos, acuerdos y las responsabilidades asignadas.
2.7 Mejoraré la comprensión por la comunidad de la informática y sus consecuencias.
2.8 Accederé a los recursos de comunicación e informática sólo cuando se esté autorizado a hacerlo.

3. Obligaciones de liderazgo organizativo

3.1 Articularé las responsabilidades sociales de los miembros de una unidad organizativa y fomentaré la completa aceptación de esas responsabilidades.
3.2 Gestionaré personal y recursos para diseñar y construir sistemas de información que mejoren la calidad, efectividad y dignidad de la vida laboral.
3.3 Reconoceré y apoyaré los usos adecuados y autorizados de los recursos informáticos y de comunicaciones de la organización.
3.4 Garantizaré que los usuarios y aquellos que se verán afectados por el sistema informático han articulado claramente sus necesidades durante la evaluación y el diseño de los requisitos. Después el sistema debe ser validado para cumplir los requisitos.
3.5 Articularé y apoyaré las políticas que protegen la dignidad de los usuarios y de quienes se vean afectados por el sistema informático.
3.6 Crearé condiciones para que los miembros de la organización aprendan los principios y limitaciones de los sistemas informáticos.

4. Conformidad con el código

4.1 Defenderé y promoveré los principios de éste código.
4.2 Trataré los incumplimientos de este código como inconsecuentes con la afiliación a la ACM.

5.3.5 Código de ética desarrollado por el comité conjunto IEEE-CS/ACM en Ética y Ejercicio Profesional de Ingeniería de Software (SEEPP):

Los ingenieros de software deberán comprometerse consigo mismo en convertir el análisis, especificación, diseño, desarrollo, prueba y mantenimiento de software en una profesión respetable y beneficiosa. Principio de acuerdo con su compromiso con la salud, seguridad y bienestar del público, los Ingenieros de Software deberán apegarse a los siguientes Ocho Principios:

1. ***PUBLICO*** - Los Ingenieros de Software deberán actuar consistentemente con el interés público.

2. ***CLIENTE Y EMPLEADOR*** - Los Ingenieros de Software deberán actuar de una forma determinada que esté en los mejores intereses de su cliente y empleador consistente con el interés público.

3. ***PRODUCTO -*** Los Ingenieros de Software deberán asegurar que sus productos y modificaciones relacionadas logren el más alto estándar profesional posible.

4. ***JUICIO*** - Los Ingenieros de Software deberán mantener integridad e independencia al emitir su juicio profesional.

5. ***GERENCIA*** - Los gerentes y líderes de Ingeniería de Software deberán suscribirse y promocionar un enfoque ético para la gerencia de desarrollo y mantenimiento de software.

6. ***PROFESION*** - Los Ingenieros de Software deberán fomentar la integridad y reputación de la profesión consistente con el interés público.

7. ***COLEGAS*** - Los Ingenieros de Software deberán ser justos y comprensivos con sus colegas.

8. ***INTERES PROPIO*** - Los Ingenieros de Software deberán participar en el aprendizaje de por vida del ejercicio de su profesión y deberán promover un enfoque ético para el ejercicio de la misma.

5.3.6 Ética en Internet (Ciberespacio)

Internet es el último y el más poderoso de una serie de medios de comunicación (telégrafo, teléfono, radio y televisión) que durante el último siglo y medio ha eliminado progresivamente el tiempo y el espacio como obstáculos para la comunicación entre un gran número de personas.

Como sucede con otros medios de comunicación, la persona y la comunidad de personas son el centro de la valoración ética de Internet. Con respecto al mensaje comunicado, al proceso de comunicación y a las cuestiones estructurales y sistemáticas de la comunicación

La cuestión ética consiste en saber si esto está contribuyendo al auténtico desarrollo humano y ayudando a las personas y a los pueblos a ser fieles a su destino trascendente, "el principio ético fundamental es el siguiente: la persona humana y la comunidad humana son el fin y la medida del uso de los medios de comunicación social; la comunicación debería realizarse de persona a persona, con vistas al desarrollo integral de las mismas".

Internet tiene un conjunto de características impresionantes como lo describimos a continuación:

- Instantáneo.
- Inmediato.
- Mundial.
- Descentralizado.
- Interactivo.

Capaz de extender ilimitadamente sus contenidos y su alcance, flexible y adaptable en grado notable. Puede emplearse para romper el aislamiento de personas y grupos o al contrario, para profundizarlo. Internet le sirve a la gente en su ejercicio responsable de la libertad y la democracia, ampliar la gama de opciones realizables en diversas esferas de la vida, ensanchar los horizontes educativos y culturales, superar las divisiones y promover el desarrollo humano de múltiples modos.

5.3.6.1 Los problemas éticos más significativos en Internet

En gran medida el desarrollo científico y tecnológico se desarrolla día a día, por lo que debemos adaptarnos a él, pero una de las causas que generan inquietud es la vida privada, debido al gran almacenamientos de datos que se encuentran en las diferentes bases de datos y que a causa del aumento de las técnicas de búsqueda en la red (minería de datos) o en bases de datos, se encuentran en peligro debido a que dicha información pueda estar a disposición de personas no autorizadas.

Así mismo debido a éstos avances ahora es posible, en muchos campos de trabajo, que gran parte del mismo puedan realizarse desde diferentes sitios y no necesariamente en la oficina, por lo que tiene tanto ventajas como desventaja, en cuanto ventajas, podemos mencionar que se reduce la cantidad de tiempo y de dinero que se realiza de trayecto de la casa a la oficina, pero como desventaja podemos ver que se pierde las relaciones humanas, debido a que ya no existe el contacto con la gente y que como seres humanos necesitamos de las relaciones sociales para poder desempeñarnos mejor.

Un problema más a mencionar es la cantidad de información que nos brinda internet en donde hay que saber discernir entre las diferentes fuentes de información, evaluarlas y determinar si son verdaderas y reales, ya que de lo contrario nos estaríamos mal informando. Por ellos es necesario la creación de sitios seguros, donde la información este respaldada y que además se informe responsablemente a los usuarios de las diferentes amenazas y vulnerabilidades que existen, de esta manera los usuarios podrán crearse un criterio más amplio y así descubrir, usar y evaluar las fuentes de información que posibiliten su desarrollo, tanto profesional como humano.

CAPÍTULO 6

Herramientas de Seguridad Informática

En este capítulo se muestra un listado de diferentes Herramientas de Seguridad Informática que existe, donde se indica las características principales de cada una de ellas, como son el sistema operativo sobre el cual trabaja, si trabajan sobre línea de comandos o a través de una interfaz gráfica y además de indicar el tipo de Servicio de Seguridad Informática que resguarda.

CAPÍTULO 6

Herramientas de Seguridad Informática

Las herramientas que se utilizan para brindar seguridad informática son muy diversas y requieren no únicamente del tipo de aplicación o seguridad que proporcionan, sino que además las podemos identificar a través de cierta simbología, de acuerdo a la página web: http://sectools.org/, pueden utilizarse los siguientes íconos para identificar las características de cada una de las herramientas listadas:

 Generalmente, cuesta dinero. Rara vez se incluye el código fuente. Quizás haya una versión "de demostración"/limitada/gratis disponible.

 Funciona sobre Linux.

 Funciona sobre FreeBSD/NetBSD/OpenBSD y/o sistemas UNIX no-libres (Solaris, HP-UX, IRIX, etc.).

 Soporta Microsoft Windows.

↑/↓Ranking de popularidad ↑aumento / ↓bajo desde la lista del 2003.

 Soporta Apple Mac OS X

 Funciones en la interface de línea de comando

 Ofrece una interface GUI (apunta y click)

 Código fuente disponible para su inspección.

CA Control de acceso

I Integridad

C Confidencialidad

NR No repudio

A Autenticación

D Disponibilidad

#1 **Nessus :** Es, según sectools.org, la mejor herramienta de análisis de vulnerabilidades de red existente en el mercado. Posee más de 11 mil plugins gratuitos para complementar sus capacidades. Incluye revisiones locales y remotas de sistema, arquitectura de cliente/servidor en modo gráfico, y la posibilidad de escribir plugins propios en un lenguaje embebido. La última versión de Nessus (3.0) ya no es gratuita, pero se pueden seguir utilizando versiones anteriores sin costo.

CA, I, C, NR, A, D

#2 **Wireshark :** Antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos

CA, I, C,A

#3 **Snort :** 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 lo es MySQL. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida. Así mismo existen herramientas de terceros para mostrar informes en tiempo real (ACID) o para convertirlo en un Sistema Detector y Preventor de Intrusos.

CA, I, C, A

#4 **Netcat :** Netcat (a menudo referida como la navaja multiusos de los hackers) es una herramienta de red bajo licencia GPL (en la versión de GNU) disponible para sistemas UNIX, Microsoft y Apple que permite a través de intérprete de comandos y con una sintaxis muy sencilla abrir puertos TCP/UDP en un HOST (quedando netcat a la escucha), asociar una shell a un puerto en concreto (para conectarse por ejemplo a MS-DOS o al intérprete bash de Linux remotamente) y forzar conexiones UDP/TCP (útil por ejemplo para realizar rastreos de

puertos o realizar transferencias de archivos bit a bit entre dos equipos).

CA, A, C,

#5 **Metasploit Framework :** Es toda una plataforma pensada para el desarrollo de herramientas de seguridad. Se utiliza, principalmente, para la realización de tests de intrusión en redes o en servidores. Esto permite conocer las deficiencias de seguridad de estos sistemas y poder solucionarlos antes de que los descubran otros atacantes con intenciones algo más oscuras.

CA, C, AE

#6 **Hping2 :** Hping2 ensambla y envía paquetes de ICMP (Internet Control Message Protocol)/UDP (User Datagram Protocol)/TCP (Transmission Control Protocol) hechos a medida y muestra las respuestas. Fue inspirado por el comando "ping", pero ofrece mucho más control sobre lo enviado. También tiene un "modo traceroute" muy útil y soporta fragmentación de IP (Internet Protocol).

Esta herramienta es particularmente útil al tratar de utilizar funciones como las de "traceroute/ping" o analizar de otra manera, "hosts" detrás de un "firewall" que bloquea los intentos que utilizan las herramientas estándar. Plataforma: Unix y Linux.

CA

#7 ↑10 **Kismet :** Es un programa para Linux que permite detectar redes inalámbricas (WLANs) mediante la utilización de tarjetas wireless en los estándar 802.11a, 802.11b y 802.11g, en la mayoría de las que se comercializan actualmente.

CA, I, C, A

#8 ↓3 **Tcpdump :** Es un herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar a tiempo real de los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado. Tcpdump funciona en la mayoría de los sistemas operativos UNIX: Linux, Solaris,

BSD, Mac OS X, HP-UX y AIX entre otros. En esos sistemas, tcpdump hace uso de la librería libpcap para capturar los paquetes que circulan por la red.

CA, I, C, A,

#9 ↑23 **Cain and Abel :** Cain y Abel es una herramienta enfocada principalmente a la recuperación de contraseñas utilizando para esto distintos medios. Permite sniffear la red en busca de contraseñas, recupera los passwords de internet explorer, conexión telefónica, red inalámbrica, cuenta con un excelente crackeado que permite decodificar gran cantidad de contraseñas, permite ver detrás de los asteriscos "**"en contraseñas guardadas, es una excelente herramienta para entornos windows.

CA, I, C, A

#10 ↑1 **John the Ripper :** Es un programa de criptografía que aplica fuerza bruta para descifrar contraseñas. Es capaz de romper varios algoritmos de cifrado o hash, como DES, SHA-1 y otros.

Es una herramienta de seguridad muy popular, ya que permite a los administradores de sistemas comprobar que las contraseñas de los usuarios son suficientemente buenas.

John the Ripper es capaz de autodetectar el tipo de cifrado de entre muchos disponibles, y se puede personalizar su algoritmo de prueba de contraseñas. Eso ha hecho que sea uno de los más usados en este campo.

CA

#11 ↓2 **Ettercap :** es un interceptor/sniffer/registrador para LANs con switch. Soporta disecciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle(Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing.

CA, A

#12 ↑4

Nikto : Es un escaneador para servidores web realizado en lenguaje Perl, tiene licencia Open Source GPL y realiza todo tipo de pruebas de ataques y vulnerabilidades por medio de un extensible sistema de plugins.

Nikto puede ser un excelente punto de partida para comprobar la seguridad del servidor web a nuestro cargo, que funciona tanto en Linux como en Windows y tiene una gran base de datos de ataques (CGI y otros) en 230 tipos de servidores distintos.

CA, I, C, A

#13 **Ping/telnet/dig/traceroute/whois/netstat :** Se tratan de utilidades que comprueban el estado de la conexión con uno o varios equipos remotos por medio de los paquetes de solicitud de eco y de respuesta de eco (definidos en el protocolo de red ICMP) para determinar si un sistema IP específico es accesible en una red. Es útil para diagnosticar los errores en redes o enrutadores IP.

CA

#14 ↓2

OpenSSH / PuTTY / SSH : Es un conjunto de aplicaciones que permiten realizar comunicaciones cifradas a través de una red, usando el protocolo SSH. Fue creado como una alternativa libre y abierta al programa Secure Shell, que es software propietario. El proyecto está liderado por Theo de Raadt, de Calgary.

CA, I, C, A

#15 ↑35

THC Hydra : Cracker de autenticación de red paralelizado. Esta herramienta permite realizar ataques por diccionario rápidos a sistemas de entrada (login) por red, incluyendo FTP (File Transfer Protocol), POP3 (Post Office Protocol 3), IMAP (Internet Message Access Protocol), Netbios (Network Basic Input/Output System), Telnet, HTTP (HyperText Transmission Protocol) Auth, LDAP (Lightweight Directory Access Protocol), NNTP (Network News Transfer Protocol), VNC (Virtual Network Computing), ICQ ("I Seek You"), Socks5, PCNFS y más. Incluye soporte para SSL (Secure Sockets Layer).

A

#16 **Paros proxy :** Paros proxy es una aplicación para evaluación de vulnerabilidades sobre aplicaciones web. Consiste en un proxy realizado en Java que permite visualizar en tiempo real los paquetes HTTP/HTTPS y ver los elementos que se están editando o modificando, como las cookies y campos de formularios. Además, incluye un registro de tráfico, calculadora de hash y un escáner para probar ataques comunes a aplicaciones web como XSS (cross-site scripting) e inyección de SQL.

I, C, NR, A

#17 ↓10 **Dsniff :** Es una herramienta relacionada con el sniffeo. Tiene utilidades que:

- Logean conversaciones IM
- Muestra url que los clientes de la red estan viendo
- Permite sniffear conecciones https con la tecnica man in the middle(envia certificador ssl propios esperando que el usuario no sea cuidadoso).

CA, A

#18 ↑7 **NetStumbler :** Netstumbler es un programa para Windows que permite detectar WLANs usando tarjetas wireless 802.11a, 802.11b y 802.11g. Tiene varios usos, como:

1.- Verificar que la red está bien configurada.

2.- Estudiar la cobertura o señal que se tiene en diferentes puntos del domicilio de la red.

3.- Detectar otras redes que pueden causar interferencias a la red.

4.- Es muy útil para orientar antenas direccionales cuando se quiere hacer enlaces de larga distancia, o simplemente para colocar la antena o tarjeta en el punto con mejor calidad de la señal.

5.- Sirve para detectar puntos de acceso no autorizados (Rogue AP's).

6.- Por último, también nos sirve para WarDriving, es decir, detectar todos los APs que están alrededor.

CA, I, D

#19 ↑18

THC Amap : Amap es una gran herramienta para determinar que aplicación se está escuchando en un puerto dado. Sus bases de datos no son tan grandes con las que utilizan Nmap, pero es definitivamente valioso tratarla como una segunda opinión o sí Nmap falla para detectar un servicio. Amap sabe cómo analizar el rendimiento de los archivos Nmap.

CA

#20 ↓12

GFI LANguard : GFI LANguard Network Security Scanner (N.S.S.) es una solución que permite escanear, detectar, evaluar y remediar cualquier vulnerabilidad de seguridad en la red. Como administrador, a menudo se tiene que tratar diferentemente problemas relacionados con problemas de seguridad, administración de parches y auditoría de red, a veces utilizando varios productos. Sin embargo, con GFI LANguard N.S.S., esos tres pilares de la administración de vulnerabilidad son abordados en un paquete. Utilizando una única consola con amplias funcionalidades de generación de informes, la solución integrada GFI LANguard N.S.S. ayuda a abordar estos asuntos más rápida y eficazmente.

CA, I, C, A, D

#21

Aircrack : Es un programa crackeador de claves 802.11 WEP y WPA/WPA2-PSK. Aircrack-ng puede recuperar la clave WEP una vez que se han capturado suficientes paquetes encriptados con airodump-ng. Este programa de la suite aircrack-ng lleva a cabo varios tipos de ataques para descubrir la clave WEP con pequeñas cantidades de paquetes capturados, combinando ataques estadísticos con ataques de fuerza bruta. Para crackear claves WPA/WPA2-PSK, es necesario usar un diccionario.

CA, A

#22 ↓4

Superscan : Es un potente scaner de puertos, realiza pings y resuelve nombres de dominio. Realiza todo tipo de operaciones de escaneo de puertos usando una IP o un fichero de texto del cual extraer las mismas. Es capaz de conectar a cualquier tipo de puerto que se descubra, usando aplicaciones apropiadas (Telnet, FTP, Web).**CA**

#23 **Netfilter :** Es un servicio completo de Administración de Accesos y Filtrado de Contenido de Internet, que elimina páginas de pornografía, drogas y violencia garantizando un alto nivel de seguridad a sus usuarios.

El sistema es presentado en las modalidades PC (para ordenadores aislados y pequeñas redes) y Red (para redes con más de 15 ordenadores). En esta última versión, además del filtrado, también es ofrecida una completa solución de seguridad y monitoreo de accesos.

CA, A

#24 **Sysinternals :** es un conjunto de utilidades o suite de herramientas para sistemas Windows 95 / 98 / Me / 2000 / NT / XP / 2003 / Vista, que han sido reunidas en un único archivo de descarga de 8Mb.

CA, I, A

#25 **Retina :** este programa es un conocido scanneador de vulnerabilidades que es comercial y que incluye la forma de arreglar todos los agujeros de seguridad que encuentre. Es para Windows.

CA

#26 **Perl / Python / Ruby :** Son lenguajes de scripts que corren en cualquier sistema operativo y que sirve, entre otras múltiples cosas, para crear exploits y explotar las vulnerabilidades de los sistemas.

CA, I, C, A

#27 **L0phtcrack :** Es una aplicación para recuperación de contraseñas que permite a los administradores reducir sus riesgos, ayuda a identificar y remediar fallos de seguridad causados por contraseñas débiles o fáciles de adivinar y a acceder a cuentas de usuario o administrador de Windows y Unix cuyas contraseñas se han perdido. Además algunas versiones de L0phtCrack permiten utilizar listas de contraseñas prefabricadas (tipo raimbowcrack) que cubren trillones de posibilidades.

CA, A

#28 **Scapy :** Herramienta de manipulación de paquetes interactiva, generación de paquetes y descubrimiento de red.

I, C, A

#29 **Sam Spade :** Herramienta útil para la exploración, administración y seguridad de red. Incluye múltiples herramientas útiles.

↓16

CA, A

#30 **GnuPG / PGP :** substituto del PGP con licencia GNU desarrollado en Europa que no utiliza ni el algoritmo RSA ni IDEA y que por ello no tiene ningún tipo de restricción. PGP o Pretty Good Privacy es el famoso sistema de encriptación que ayuda a asegurar y codificar la información contra posibles "escuchas".

I, C, A

#31 Airsnort : es una herramienta de seguridad para GNU/Linux y Windows, escrita en GTK+ por Blake Hegerle y Jeremy Bruestle, que sirve para decifrar las claves WEP en una red 802.11b. Esta herramienta surgió como la inspiración sobre las vulnerabilidades descritas por el documento *Weaknesses in the Key «Scheduling Algorithm of RC4»* escrito por Scott Fluhrer, Itsik Mantin and Adi Shamir (este último, uno de los inventores del algoritmo RSA). Airsnort solo requiere recolectar de cinco a diez millones de de paquetes cifrados desde un punto de acceso inalámbrico para poder recuperar una clave WEP, por lo que es una buena forma de poner a prueba la seguridad y decidirse a cambiar a WPA. Está disponible, en su versión 0.2.7e, a través de los depósitos de equipamiento lógico de AL Desktop para CentOS 5**,** Red Hat Enterprise Linux 5 y White Box Enterprise Linux 5.

↓3

CA, A

#32 **BackTrack :** Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en el entorno de la seguridad informática.

CA, I, C, NR, A, D

#33 **P0f :** Es una herramienta para obtener información remota sobre el sistema operativo y versiones de servidor de una máquina. Su principal característica es que no deja huella en los firewalls y sistemas de detección de intrusos (a diferencia de escáneres de puertos activos como Nmap).

CA, A

#34 **Google :** Google Hacking se trata de una forma de obtener información privada aprovechando el poder de indexación del buscador Google.

CA

#35 **WebScarab :** Práctica aplicación programada en Java, que permite analizar de forma eficaz y segura programas que se comuniquen utilizando protocolos HTTP y HTTPS. WebScarab forma parte del proyecto OWASP (Open Web Application Security Project), una interesante iniciativa para la creación de aplicaciones seguras y fiables de código abierto. Gratuito, el programa está disponible solamente en inglés.

CA, C, A

#36 ⬆3 **Ntop :** NTOP (Network TOP) es una herramienta que no puede faltar al administrador de red, porque permite monitorizar en tiempo real los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto y además es capaz de ayudarnos a la hora de detectar malas configuraciones de algún equipo (esto salta a la vista porque al lado del host sale un banderín amarillo o rojo, dependiendo si es un error leve o grave), o a nivel de

servicio. Posee un microservidor web que permite que cualquier usuario, que sepa la clave, pueda ver la salida NTOP de forma remota con cualquier navegador, y además es GNU. El software está desarrollado para platarfomas Unix y Windows.

CA, A

#37 ↓22 **Tripwire :** Es un programa de computador Open Source consistente en una herramienta de seguridad e integridad de datos. Tripwire es útil para monitorizar y alertar de cambios específicos de ficheros en un rango de sistemas. Para mejor eficacia, se recomienda instalar el programa antes de haber conectado la computadora por primera vez a internet a fin de crear una base de datos de los ficheros existentes en el sistema, para poder contrastar los posibles cambios en éstos una vez conectado a la red. Tripwire funciona correctamente en sistemas operativos GNU/Linux.

CA, I, C, A

#38 ↓3 **Ngrep :** Es un 'grep' para el tráfico de red. Ngrep se esfuerza por proveer de la mayoría de características comunes del 'grep' de GNU, aplicándolas a la capa de red. Ngrep es consciente de la presencia de 'pcap' y te permite usar expresiones regulares que concuerden con el 'payload' (la carga) de los paquetes. Actualmente reconoce TCP, UDP, e ICMP sobre Ethernet, PPP, SLIP e interface nulas ('null interfaces'), y comprende la lógica de un flitro 'bpf' de la misma manera que herramientas más comunes de sniffing como 'tcpdump' y 'snoop'.

CA, A

#39 ↓10 **Nbtscan :** Es un escáner de nombres NetBIOS en la red que recolecta información mandando peticiones de estado a las máquinas conectadas a la red. Soporta los sistema operativos de Unix / Linux / Windows (testeado en NT4 y 2000).

CA

#40 **WebInspect:** Es un producto de SPI Dynamics que permite revisar y detectar vulnerabilidades en aplicaciones Web. WebInspect es capaz de revisar código de aplicaciones emergentes orientadas a la Web 2.0, con empleo de tecnologías como AJAX, SOAP, SOA, JavaScript y Flash.

CA, I, C, NR, A, D

#41 **OpenSSL :** Es un proyecto de software desarrollado por los miembros de la comunidad Open Source para libre descarga y está basado en SSLeay desarrollado por Eric Young y Tim Hudson. Consiste en un robusto paquete de herramientas de administración y librerías relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS). Estas herramientas ayudan al sistema a implementar el Secure Sockets Layer (SSL), así como otros protocolos relacionados con la seguridad, como el Transport Layer Security (TLS). Este paquete de software es importante para cualquiera que esté planeando usar cierto nivel de seguridad en su máquina con un sistema operativo Libre basado en GNU/Linux. OpenSSL también nos permite crear certificados digitales que podremos aplicar a nuestro servidor, por ejemplo Apache.

3

CA, I, C, A

#42 **Xprobe2 :** Xprobe2 permite determinar qué sistema operativo se está ejecutando en un servidor remoto. Envía varios paquetes a un servidor y analiza las respuestas.

9

La funcionalidad de Xprobe2 es comparable a la característica de huellas de SO de nmap (escrita por un Fyodor distinto):

- Muestra el nivel de confianza sobre el SO del servidor remoto.
- Sigue funcionando aunque sistemas intermedios (enrutadores, cortafuegos) hagan pequeñas modificaciones a los paquetes.
- Puede listar el tipo de dispositivo intermedio (por ejemplo: «Linux IP masquerading»).
- La arquitectura modular le permite añadir nuevas pruebas de huellas y firmas de SO

CA, A

#43 **EtherApe :** Es un sistema de monitorización gráfica para la red.

21

Muestra la actividad de la red gráficamente. Los hosts y links cambian su tamaño en relación al tráfico que en ese momento sea latente. También diferencia los protocolos mediante colores.

Es capaz de filtrar el tráfico que debe ser mostrado y de mostrar directamente el tráfico de un fichero como si fuese directamente de la red.

CA, A

#44 **Core Impact :** Es el producto más exhaustivo para evaluar la seguridad a nivel corporativo.

Integra el testeo de servidores, sistemas de escritorios, de usuarios y aplicaciones web contra amenazas reales a la seguridad de la información. Esto permite aprovechar el servidor como un "puesto de avanzada" desde donde ejecutar pruebas automatizadas de penetración de redes contra otros sistemas en la red, como podría hacer un atacante. Comprender cómo las vulnerabilidades –en las diferentes capas de la red y explotadas mediante diferentes vectores de ataques– pueden ser combinadas para construir trayectorias de ataques en una organización, es invaluable para concebir efectivos mecanismos de mitigación.

CA, C, A

#45 **IDA Pro :** IDA Pro es un desensamblador, capaz de realizar la ingeniería inversa de casi cualquier programa hecho para casi cualquier procesador.

#46 ↓12 **SolarWinds :** SolarWinds TFTP Server instala un servicio TFTP habitualmente usado para transferencias de archivos pequeños en una red.

El protocolo TFTP (Trivial File Transfer Protocol) Protocolo de transferencia de archivos trivial, se parece al FTP aunque le diferencia que sólo lee y escribe archivos, no utiliza cifrado y cada archivo enviado supone un intercambio independiente de paquetes.

CA

#47 ↑6 **Pwdump :** Herramienta fundamental en la seguridad de redes Windows que permite extraer los LM Hashes encriptados para crackearlos y obtener las contraseñas de los usuarios de Windows. Funciona en línea de comandos y permite extraer estos hashes de forma remota (con el password de administrador). Versión antigua, aunque es la más utilizada de los últimos años.

CA

#48 ↓7 **LSoF :** es una conocida herramienta de detección de intrusión en sistemas, que nos muestra todos los archivos que mantiene abiertos un determinado ID de proceso (PID), incluyendo los sockets abiertos.

Proporciona una lista de todos los puertos que estén abiertos y demás información adicional. Si no se indica ninguna opción restrictiva, lsof enumera todos los archivos abiertos en ese momento, que normalmente suelen ser bastantes.

CA, I, C, A

#49 **RainbowCrack :** Es un crackeador de hashes entre los cuales puede crackear NTLM, MD2, MD4 and RIPEMD160 usando el método de fuerza bruta funciona a través de unas tablas que podemos generar a nuestro en tamaño caracteres etc.

CA

#50 ↓19 **Firewalk** : Es un cortafuego flexible, completo y perfectamente integrado a Mac OS X, con numerosas funciones como el acceso Internet restringido para ciertas aplicaciones especificas o alarmas en tiempo real para intentos de intrusión.

CA, A

#51 **Angry IP Scanner** : Es una pequeña herramienta que analiza y monitoriza el estado de las direcciones IP en una red local.

Puede analizar cualquier IP para comprobar si responde, resolver el nombre de host e intentar conectar con aquellas que especifiques en el diálogo de configuración.

El programa utiliza diferentes hilos de conexión para cada IP para reducir el tiempo de espera, y muestra también información general sobre el PC como el nombre de la máquina, su grupo de trabajo en red y nombre del usuario que está conectado.
CA, A

#52 **RKHunter :** Es una herramienta de Unix que detecta los rootkits, los backdoors y los exploit locales mediante la comparación de los hashes MD5 de ficheros importantes con su firma correcta en una base de datos en línea, buscando los directorios por defecto (de rootkits), los permisos incorrectos, los archivos ocultos, las cadenas sospechosas en los módulos del kernel, y las pruebas especiales para Linux y FreeBSD.

CA, I, C, NR, A

#53 **Ike-scan :** Es una herramienta de comprobación para dispositivos que permitan abrir túneles VPN. Permite identificar el producto de forma remota.

A

#54 ↑21 **Arpwatch :** Es un paquete formado por arpwatch y arpsnmp, dos utilidades que nos serán de gran ayuda para monitorizar el tráfico de red y generar al vuelo unas bases de datos de direcciones pares Ethernet/IP, reportando de esta forma los cambios ocurridos en todo momento.

Arpwatch NG está basado en el paquete original del mismo nombre, aunque éste es más moderno y adaptado a las tecnologías actuales. Así, permite monitorizar direcciones MAC en una red, y escribirlas en tablas que guarda en un fichero. Incluye registro timestamp y un sistema de notificación de cambios.

Es ideal para comprobar las correspondencias entre pares IP/Mac de una red, ya que en caso de que se produzca un cambio en un par, se recibirá una notificación por correo electrónico del suceso a la cuenta de administrador del sistema. De la misma forma, sirve también para monitorizar nuevas direcciones Mac en la red.

CA, A

#55 **KisMAC :** Es un stumbler, es decir un rastreador capaz de pasar la tarjeta Airport en modo monitor y detectar todas las redes inalámbricas disponibles en tus cercanías, y controlar el tráfico que se realiza a través de ellas.

KisMAC está desarrollado totalmente bajo una licencia abierta GPL y funciona con las tarjetas Airport o tarjetas PCMCIA con chipset Oricono o Prism2. No solamente

permitirá conocer el perímetro de la red inalámbrica y controlar todo el tráfico, sino también detectar redes cercanas y obtener información de ellas.

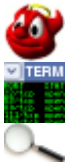
KisMAC, a la diferencia de sus homólogos, actúa de forma totalmente transparente y permite observar nodos de conexión de redes inalámbricas, así como conectarse a nodos con buena señal.

CA, A, D

#56 **OSSEC HIDS :** Funciona como un sistema de detección de intrusos, y entre sus herramientas realiza exhaustivos análisis, es capaz de responder activamente, cuenta con alertas temporales, y muchas cosas más. Es gratuito, el programa está disponible en inglés, alemán, italiano, polaco, portugués y turco.

CA, I, C, A

#57 ↑4 **Openbsd PF :** Usa un algoritmo de cifrado de contraseñas derivado del Blowfish de Bruce Schneier. Este sistema se aprovecha de la lentitud inherente del cifrado del Blowfish para hacer la comprobación de contraseñas un trabajo muy intensivo para la CPU, dificultando sobremanera el procesamiento paralelo. Se espera que así se frustren los intentos de descifrado.



CA

#58 ↓18 **Nemesis :** El Proyecto Nemesis está diseñado para ser una pila de IP ("IP stack"), portable y basada en línea de comandos para UNIX/Linux. El set está separado por protocolos, y debería permitir crear scripts útiles de flujos de paquetes inyectados desde simples scripts de shell.

CA, A

#59 **Tor :** Es una herramienta gratuita que permite que la gente utilice Internet de manera anónima. Básicamente, ingresando a Tor se ingresa a una red de computadoras alrededor del mundo que pasan el tráfico de Internet entre todas ellas de manera aleatoria antes de enviarla fuera, a dónde sea que el mismo se dirija. Imagínese un grupo con muchas personas pasándose cartas entre ellas. En algún momento, la carta abandona ese grupo y se envía a algún destinatario.

CA, D

#60 **Knoppix :** Es una distribución de GNU/Linux basada en Debian y que por defecto utiliza KDE aunque en el menú de arranque se puede especificar el tipo de interface grafica a usar (Gnome, IceWM, ...). Está desarrollada por el consultor de GNU/Linux Klaus Knopper. Knoppix es conocido por sus maravillosas capacidades de detección de hardware. Ya que debería detectar la mayoría de las tarjetas de vídeo y tarjetas de sonido.

A

#61 **ISS Internet Scanner :** Internet Security Scanner es una herramienta comercial de análisis de vulnerabilidades para Windows.

INTERNET SECURITY SYSTEMS®

CA, A

#62 **Fport :** Reporta todos los puertos, TCP/IP y UDP abiertos en la máquina en la que es ejecutado y muestra qué aplicación abrió cada puerto y sus aplicaciones asociados. Sólo funciona bajo Windows.

CA, A

#63 **chkrootkit :** Es un programa informático para consola común en sistemas operativos Unix y derivados que permite localizar rootkits conocidos, realizando múltiples pruebas en las que busca entre los ficheros binarios modificados por dicho rootkit. Este guión de consola usa herramientas comunes de UNIX/Linux como las órdenes strings y grep para buscar las bases de las firmas de los programas del sistema y comparar un transversal del archivo del sistema /proc con la salida de la orden ps (estado de los procesos (process status)) para buscar discrepancias. Básicamente chkrootkit hace múltiples comprobaciones para detectar todo tipo de rootkits y ficheros maliciosos.

chkrootkit

CA, I, C, NR, A

#64 **SPIKE Proxy :** Es un proxy de HTTP "open source" que sirve para encontrar fallas de seguridad en sitios web. Es parte del Spike Application Testing Suite y soporta detección de inyección de SQL automatizada, crawling *** de sitios web, uso de fuerza bruta en formularios de entrada,

IMMUNITY

detección de overflow, y detección de acceso a directorios que debieran estar fuera de los límites del sitio de web {"directory traversal"}.

A

#65 ↓14 **OpenBSD :** Es un sistemas Operativos de tipo BSD, como los conocidos FreeBSD y NetBSD. Es compatible con muchas de las arquitectura que se conoce en el mercado, tal es el caso de Intel, AMD, ARM, Sparc, Digital, sgi, Motorola, Mac, Zaurus, entre los más reconocidos de las casi 17 soportadas. Principalmente el diseño y la implementación de OpenBSD se basa en NetBSD.

Uno de los puntos más fuertes de OpenBSD se enfoca principalmente en la seguridad y los mecanismos de criptografía, esto es tan así que uno de los principales usos o por lo menos los más conocidos es como Firewall utilizando su herramienta nativa PF y como terminador de Túneles Virtuales conocidos como VPN, gracias a la herramienta IPSec, la cual ya está incorporado en su kernel.

CA, I, C, A

#66 **Yersinia :** Es una herramienta para verificar la correcta configuración y seguridad de los dispositivos de red. Es una herramienta distribuida bajo la licencia GPL, por lo que cualquier persona puede utilizarla respetando su licencia de uso y distribución, siendo una de las aportaciones de S21sec a la comunidad del software libre.

CA, A, D

#67 **Nagios :** Es una herramienta de monitorización bajo licencia GNU versión 2. Monitorea hosts, servicios, routers, recursos, factores ambientales, cualquier cosa que definamos. Posee un diseño simple que permite desarrollar fácilmente plugins personalizados. Es flexible, nos permite definir entre otras cosas que son para nosotros una alerta o no. Informa en tiempo real (email, SMS, jabber) problemas de red, antes que los clientes, usuarios finales o jefes los noten. Posee una interfaz web sencilla que nos permite ver el status actual de la red, las notificaciones, hacer reportes, ver historicos, etc.

CA, I, C, A, D

#68 ↓20 **Fragroute/Fragrouter :** Permite *"interceptar, modificar y reescribir tráfico destinado a un host específico, permitiendo insertar la mayoría de los ataques conocidos"* Es un router fragmentador de una vía– los paquetes IP son enviados

desde el atacante al Fragrouter, el cual los transforma en streams de datos fragmentados para enviarlos a la víctima. Muchos IDS de red no son capaces o simplemente no se molestan en reconstruir una vista coherente de los datos de red. Fragrouter ayuda a los atacantes a lanzar ataques basados en red evitando su detección. Es parte de la suit de herramientas NIDSbench de Dug Song, Fragroute es una herramienta similar del mismo autor.

CA, A

#69 **X-scan :** Es un scanner de vulnerabilidades que trabaja en modo multitarea con soporte de plugins. Incluye características tales como soporte NASL, detección de tipos de servicio, detección remota de versiones de sistemas operativos, y detección de pares de autenticación débiles.

CA, I, C, A, D

#70 ↓60 **Whisker/libwhisker :** Libwhisker es un módulo Perl creado para pruebas http. Provee funciones para chequear servidores http para muchos agujeros de seguridad, particularmente la presencia de CGIs peligrosos. Whisker es un escáner que usa libwhisker pero que está quedando en desuso a favor de Nikto que también usa este módulo.

CA

#71 **Socat** : Es una herramienta muy similar a Netcat que trabaja sobre un número de protocolos y a través de archivos, dispositivos, y sockets, además de tener un cliente para SOCKS4, un proxy CONNECT o SSL, entre otras cosas. Provee distintos modos para comunicación de interprocesos, y muchas otras opciones. Puede ser usado, por ejemplo, como un relay TCP, como una interfaz de escritorio para sockets UNIX, como un relay IPv6, para redirigir programas basados en TCP hacia una línea serial, o para establecer un ambiente relativamente seguro para correr scripts de cliente o servidor en conexiones de red.

CA, C, A

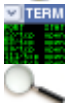
#72 ↓46 **Sara :** Es una herramienta de pruebas de vulnerabilidades derivada del scanner SATAN. Fue creado por la comunidad Open Source y posee actualizaciones quincenales.

CA, I, C, A, D

#73 **QualysGuard :** Es una herramienta que funciona como servicio Web, lo cual evita todo el proceso de instalación, mantención, y compatibilidad con sistemas operativos. Ofrece más de 5000 chequeos únicos de seguridad, un motor de búsqueda basado en inferencias y una base de conocimientos que se actualiza diariamente.

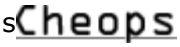
D

#74 **ClamAV :** Es una solución de antivirus de código abierto que reproduce líneas de comando para escaneo de archivos, actualizando las definiciones de antivirus y un daemon para escaneo rápido, necesario en sistemas de alta performance. A diferencia de la mayoría de los productos de antivirus, ClamAV/SOSDG no requiere suscripción anual, y es completamente gratuito bajo la licencia pública general V2.



CA, C, A

#75 **cheops / cheops-ng** : provee de una interfaz simple a muchas utilidades de red, mapea redes locales o remotas e identifica los sistemas operativos de las máquinas.



A

#76 **Burpsuite :** Es un conjunto de programas java para el análisis de servidores Web. Consta de proxy, spider, intruder y repeater. La versión gratuita está limitada, siendo la versión completa de pago.

CA, A

#77 **Brutus :** Es un crackeador de passwords remoto en línea, es rápido admite hasta 60 conexiones simultaneas (por lo que hay que tener cuidado con esto debido a

que se puede suspender algún servicio), puede llegar 2500 palabras por segundo.**CA, A**

#78 **Unicornscan :** Esta herramienta es un escáner de puertos y protocolo con gran potencia y velocidad. Es un escáner veraz que se adapta a redes muy grandes manteniendo una velocidad realmente alta. El escáner es veraz pues dice al probador exactamente qué datos se están devolviendo en un formato claro. Los resultados pueden ir a un Base de Datos SQL para que se pueda revisar y hacer un seguimiento.

CA, C, A

#79 ↓33 **Stunnel :** Es una interesante herramienta de seguridad que permite encriptar fácilmente conexiones TCP dentro de SSL. Cuenta además con más funcionalidades y herramientas para mejorar la seguridad.

CA, I, C, NR

#80 ↓37 **Honeyd :** Es un pequeño demonio que crea hosts virtuales en una red. Los hosts se pueden configurar para correr servicios arbitrarios, y su comportamiento puede ser adaptado de modo que parezcan estar ejecutándose en ciertos sistemas operativos. Honeyd permite a un solo host utilizar múltiples direcciones en un LAN para la simulación de una red. Honeyd proporciona los mecanismos para la detección y el análisis de amenazas. También disuade a los atacantes ocultando los sistemas verdaderos en medio de sistemas operativos virtuales.

CA, C

#81 ↓25 **Fping :** Es un simple programa diseñado para ser utilizado en lugar del programa ping estándar que viene con Windows. En principio fue desarrollado para enviar más de un ping por segundo.

CA

#82 **BASE :** Es un motor de análisis basado en PHP que busca y procesa una base de datos de eventos de seguridad generados por varios IDS, Firewalls, y herramientas de monitoreo de red. Entre sus características se encuentra una interfaz de búsqueda y construcción de peticiones para encontrar alertas bajo diferentes patrones, un decodificador y visor de paquetes, y cartas con estadísticas basadas en tiempo, sensor, firma, protocolo, dirección IP y otros.

CA, I, C, A

#83 **Argus :** Es un monitor de tiempo real de modelo corregido, diseñado para hacer un seguimiento y reportar el estado del rendimiento de todas las transacciones de red vistas en un stream de tráfico de datos de red. Argus provee un formato de datos común para reportar indicadores como conectividad, capacidad, demanda o retraso en una transacción. El formato utilizado por esta herramienta es flexible y extensible.

D

#84 **Wikto :** Es una completa herramienta para analizar vulnerabilidades en aplicaciones web. Permite realizar fingerprinting del servidor web, extracción de directorios y links, análisis de vulnerabilidades, ataques man-in-the-middle.

A

#85 **Sguil :** Esta herramienta está construida por los analistas de seguridad para realizar análisis de seguridad de red. Su componente principal es una interfaz gráfica que provee eventos en tiempo real desde Snort. Además incluye otros componentes que facilitan la práctica del monitoreo de seguridad de redes y análisis conducido de eventos de alertas de IDS.

CA, I, C, A

#86-39 **Scanrand :** Es un scanner de puertos y un descubridor de hosts muy similar en diseño al Unicornscan. Tranza confiabilidad por su velocidad y usa técnicas criptográficas para prevenir a los atacantes de manipular los resultados del scan.

CA, C, A

#87 **IP Filter :** Es un paquete de software que puede ser utilizado para proveer NAT o servicios de Firewall. Puede ser usado tanto como un módulo cargable al Kernel o incorporado dentro del Kernel UNIX, úselo como un módulo cargable al Kernel cada vez que sea posible.

CA, A

#88 **Canvas :** Es una herramienta de exploit de vulnerabilidades de Dave Aitel, de Inmunity Sec. Incluye más de 150 exploits y es más barato que Core Impact, pero sigue costando miles de dólares. También se puede comprar el VisualSploit plug-in para obtener una interfaz gráfica donde puede crear exploits por medio de métodos de arrastrar y colocar. En esta herramienta se suelen encontrar exploits de tipo "zero days".

CA, A

#89 **VMware :** Principalmente permiten una interacción más dinámica entre las máquinas host (anfitrion-Win XP) y guest (invitadas-Win2003, Backtrack), ofreciendo de manera simple la posibilidad de compartir archivos y carpetas, realizar drag and drops de archivos, cambios de configuración de pantalla, aceleración de dispositivos y demás.

D

#90 **Tcptraceroute :** Por medio del Envío de paquetes TCP SYN en vez de UDP o ICMP ECHO, traceroute es capaz de hacer un bypass de los filtros de Firewall más comunes.

CA, C, A

#91 ↓67 **SAINT** : Acrónimo de Security Administrator's Integrated Network Tool, es otra herramienta comercial como Nessus o Retina. Corre en Unix y solía ser grautita y Open Source, pero ahora es un producto comercial. **CA, I, C, A**

#92 **OpenVPN :** OpenVPN es un paquete SSL VPN OpenSource que puede acomodarse a una gran cantidad de configuraciones, incluyendo acceso remoto, VPNs site-to-site, seguridad WiFi, y soluciones de acceso remoto a escala de empresas, logrando balance de carga, control de fallos y controles de acceso con granularidad fina. OpenVPN implementa extensiones seguras de red en las capas OSI 2 o 3 usando el protocolo estándar de la industria SSL/TLS, soporta múltiples métodos de autenticación de cliente basado en certificados, y/o autenticación de 2 factores, y permite políticas de control de acceso para usuarios o grupos específicos usando reglas de Firewall aplicadas a la interfaz virtual de la VPN.

CA, C, A

#93 **OllyDbg :** OllyDbg analiza y optimiza aplicaciones en código binario. OllyDbg es un programa para desensamblar y debuguear programas. Posee un entorno gráfico que hace muy intuitiva y sencilla su utilización.

A

#94 **Helix :** Es una distribución personalizada de Knoppix. Es mucho más que un Live CD Booteable, puesto que contiene kernels personalizados de Linux, una excelente detección de Hardware y una gran cantidad de aplicaciones dedicadas a la respuesta a incidentes e informática forense. Fue designado con mucho cuidado para no tocar el equipo host en cualquier forma, requisito básico en la informática forense. Helix no monta ni el espacio en Swap ni los dispositivos conectados a el en forma automática. **A**

#95 ↓38 **Bastille :** El programa de Hardening Bastille "bloquea" un sistema operativo, configurando el sistema de manera proactiva para incrementar la seguridad y decrementar la susceptibilidad al compromiso. Además muestra el estado actual del hardening, reportando granularmente cada una de las configuraciones de seguridad con las que trabaja. Bastille actualmente soporta RedHat, SUSE, Debian, Gento y

Mandrake, además de HP-UX y Mac OS X. Bastille está focalizado en permitir al administrador o usuario del sistema escoger exactamente como robustecer el sistema operativo. En su sistema de hardening por defecto, pregunta interactivamente al usuario, explicando los tópicos de sus preguntas, y crea una política basada en las respuestas del usuario. Luego aplica la política al sistema. En su modo de pruebas, crea un reporte intentando enseñar al usuario sobre las configuraciones de seguridad disponibles al mismo tiempo que le informa cuales configuraciones fueron ajustadas.

CA, A

#96 **Acunetix Web Vulnerability Scanner :** Esta herramienta chequea automáticamente sus aplicaciones Web en búsqueda de vulnerabilidades como SQL Injection, Cross-Side Scripting y sistemas de autenticación de páginas débiles. Es capaz además de crear reportes de auditorías de seguridad en un sitio Web profesional.

CA, C, A

#97 **TrueCrypt :** Es un sistema de encriptación de disco OpenSource. Los usuarios pueden encriptar sistemas de archivos completos, los cuales son encriptados/desencriptados "al vuelo" como sea necesario sin la intervención del usuario más allá de ingresar su passphrase inicial. Una inteligente característica de volumen oculto permite ocultar una segunda capa de contenido particularmente sensible con las consideraciones lógicas de denegación sobre todo lo que ahí exista; de tal manera que si se ve forzado a entregar su passphrase, sólo entrega acceso al primer nivel secreto. Incluso con ello, los atacantes no pueden asegurar que un segundo nivel de encriptación exista.

C

#98 **Watchfire AppScan :** Esta herramienta provee testeo de seguridad a través del ciclo de vida del desarrollo de las aplicaciones, uniendo fácilmente el aseguramiento de calidad en cuanto a la seguridad de las aplicaciones desde su etapa de creación. Es capaz de revisar varias vulnerabilidades típicas, como Cross-Side Scripting, HTTP response splitting, parameter tampering, hidden field manipulation, opciones de backdoors/debug, buffer overflows y más.
CA, C, A

#99 ↓72 **N-Stealth :** Es un scanner de seguridad para servidores Web comercial. Es actualizado con mayor frecuencia que otros similares (como Whisker/libwhisker o Nikto). Sus afirmaciones tales como "30 mil vulnerabilidades y exploits" o "docenas de chequeos de seguridad son añadidos a diario" son muy cuestionables. Además es necesario notar que muchos de los analizadores de aplicaciones contienen componentes Web.

CA, I, C, A

#100 ↓37   **MBSA :** Microsoft Baseline Security Analyzer es una herramienta gratuita de Microsoft que permite verificar el estado de seguridad de una máquina Windows, basándose en el estado de las actualizaciones del sistema operativo y de otros productos Microsoft (esto coordinado con Microsoft Update), la configuración de Internet Explorer, el uso de cuentas y sus privilegios, y otros detalles de relevancia dentro de la configuración de seguridad del equipo.

CA, A

CONCLUSIONES

Conclusiones

Debido al surgimiento de nuevas tecnologías de la información, así como del crecimiento de las redes de comunicación, se vuelve importante la creación de un sitio web en nuestro idioma que funcione como una herramienta para la obtención de conocimientos enfocados a la Seguridad Informática. Es por esto que la presente tesis fue desarrollada de acuerdo a las necesidades descritas; en dicho portal se podrá encontrar fundamentos de seguridad informática, algunos de los diferentes estándares y esquemas de seguridad, también podrán encontrar ligas a diferentes herramientas de seguridad para contrarrestar los diferentes tipos de ataques, amenazas y vulnerabilidades.

Para ello se realizó un análisis de los diferentes tópicos que existen en seguridad informática y se desarrollaron cada uno de los temas, de tal forma que a partir del capítulo 3 se presenta la información que está contenida dentro del portal de Seguridad Informática, en dicho capítulo se da a conocer la importancia, los conceptos y fundamentos teóricos de la Seguridad Informática, el cual se vuelve uno de los capítulos más importantes debido a que es donde podemos sensibilizar al público en general sobre la importancia de la necesidad de proteger uno de los activos más importantes como es la información tanto personal como de las mismas instituciones, además de mostrar los diferentes estándares nacionales e internacionales sobre Seguridad Informática y proporcionar un panorama general de las diferentes amenazas y vulnerabilidades que se presentan en los ambientes de red y así mantener informados a los usuarios para que puedan tomar sus precauciones necesarias.

Para que una empresa u organización se desarrolle y se mantenga en su sector de negocios, es necesario que cuente con sus políticas de seguridad, ya que en éstas quedarán establecidas lo que está y lo que no está permitido realizar dentro de la organización, pero no basta con tenerlas por escrito, hay que concientizar a los usuarios de la importancia de las políticas y conseguir que las acaten además de divulgarlas, asimismo hay que hacerle un seguimiento, garantizar que estén actualizadas, y por supuesto suprimir aquellas que perdieron vigencia, debido a ello es que en el capítulo 4 se muestran las diferentes metodologías para desarrollar esquemas de seguridad y administración de la seguridad, donde se presentan las etapas y pasos necesarios para llevar a cabo cada uno de los esquemas existentes y que de esta forma sirva de guía a los usuarios para que puedan realizar cada una de ellas y así ponerlos en práctica, ya

que tan importante es contar con las políticas de seguridad así mismo es necesario contar con un plan de contingencias o plan de desastres, el cual implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento. Y así identificar las consecuencias probables o los riesgos asociados con las vulnerabilidades, y así, logren un manejo de riesgos tras la implementación y mantenimiento de controles que reduzcan los efectos de éste a un nivel aceptable; por tanto el plan de contingencia tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, suficiente y con el menor costo y pérdidas posibles.

Por lo que es esencial que la información y planes de acción de este plan, se mantengan viables y puedan ser mantenidos actualizados para poder asegurar la efectividad en el momento de su ejecución.

Todas estas acciones ayudarán a mantener un entorno seguro en cuanto a las tecnologías de información, pero si no concientizamos de su importancia a la gente que día a día hace uso de ellas, y se les demuestra que lo más importante es su apoyo, ninguna de estas acciones logrará cumplir su fin, que es el de mantener segura la información.

Dentro de este trabajo se revisó y analizó la situación actual de la Seguridad Informática en México en materia de leyes informáticas, por ello se dedica un capítulo a los aspectos legales y éticos, los cuales se encuentran contenidos en el capítulo 5, donde se presentan los principales asuntos que se deben legislar, debido a que actualmente no contamos con leyes suficientes enfocadas al tema de la seguridad de la información, ya que el proceso de creación de las leyes es largo y lento y la tecnología avanza rápidamente, fue una de las problemáticas que nos encontramos durante la elaboración de esta tesis, ya que es muy escasa la información y la variedad de libros o sitios que sustenten este tema es mínimo, por ello es importante seguir al tanto de las nuevas leyes que vayan surgiendo en materia de Seguridad Informática para que de esa forma se vaya enriqueciendo la información contendida en el portal de Seguridad Informática dentro del apartado de Aspectos legales y éticos y así promover una cultura jurídica en materia de las diferentes Tecnologías de la información para fortalecer una mejor normatividad de las empresas.

Así como uno de los objetivos es sensibilizar al público en general sobre la importancia de la Seguridad Informática, a través de la presentación de los conceptos básicos, y de los diferentes ataques, amenazas y vulnerabilidades existentes, es importante también proporcionar herramientas de seguridad que contrarresten a cada una de ellas, por ello es que se realizó un capítulo dedicado exclusivamente a Herramientas de Seguridad donde se muestran unas de tantas herramientas que se pueden utilizar, actualmente se encuentran muchas herramientas, pero la mayoría de las veces se desconoce su uso en particular y el objetivo fue presentarlas de una manera clara y sencilla para que el público en general entendiera en qué consisten, a través de una explicación breve de cada una de ellas, así como de la mención de las características más importante como son las plataformas en las que es soportada, si son de licencia libre o si requieren de algún pago, si corren en una interfaz de texto o a través de una interfaz gráfica e indicar el servicio de seguridad que ayuda a proteger, como puede ser confiabilidad, autenticación, integridad, no repudio, control de acceso y/o disponibilidad.

Es de suma importancia mantener informados a los usuarios de las diferentes noticias de Seguridad Informática, que se acontecen día a día, por ello es que se elaboró un apartado dedicado a Noticias, donde el público en general puede revisar las noticias más actuales, gracias a la utilización de los RSS, los archivos RSS son archivos generado por otros sitios web que contiene una versión específica de la información publicada en esa web, de esta forma es posible mostrar al público en general un resumen de cada una de las noticias y un enlace o URL, permitiéndole al usuario dirigirse a la página web de origen que contiene el texto completo, de esta forma se cumple el objetivo de informar al público en general sobre los diferentes temas de Seguridad Informática, sin la necesidad de que exista una persona dedicada a la actualización de las noticias.

Durante el desarrollo de la presente tesis, se fueron desarrollando uno a uno, los objetivos establecidos, pero dentro de su desarrollo nos encontramos con contenido que no se había contemplado, como fue la elaboración de videos sobre diferentes temas de Seguridad Informática, los cuales fueron realizados gracias a la colaboración de diferentes profesores de la Facultad de Ingeniería como fue el caso M. C. Alejandro Velázquez Mena, la M.C Cintia Quezada Reyes, el M. I. Alejandro Padrón Godínez y el Ing. Luis Miguel Murguía, donde se abordaron temas como la importancia de la seguridad en las redes, esquemas de seguridad, criptografía y amenazas, el cual es un material realizado con la finalidad de dar un enfoque más atractivo y sobre todo mejor informado a través de profesores que son expertos en el área.

Con ello queda concluido nuestro trabajo, el cual es el inicio de un material que puede ser mejorado y actualizado por generaciones futuras que estén interesadas en el área y que quieran añadir o mejorar cada uno de los apartados, a nosotros nos queda el compromiso con nuestra universidad de actualizar este portal por lo menos dos veces al año y que la información que se presente sea lo más reciente posible.

ANEXOS

Glosario

Accesibilidad: Es el grado en el que todas las personas pueden utilizar un objeto, visitar un lugar o acceder a un servicio, independientemente de sus capacidades técnicas o físicas.

Amenaza: Una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño en los sistemas de información, produciendo pérdidas materiales, financieras o de otro tipo. Las amenazas son múltiples desde una inundación, un fallo eléctrico o una organización criminal o terrorista. Así, una amenaza es todo aquello que intenta o pretende destruir.

Análisis de riesgos de seguridad: Es un procedimiento para estimar el riesgo de los activos de cómputo relacionados y la pérdida debido a la manifestación de las amenazas.

Ataque: Es un evento exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Autenticación: Es el servicio que trata de asegurar que una comunicación sea auténtica, es decir, verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos también sean correctos.

Backup: Es la copia total o parcial de información importante del disco duro, CD´s, bases de datos u otro medio de almacenamiento. Esta copia de respaldo debe ser guardada en algún medio de almacenamiento tecnológicamente disponible como por ejemplo *cinta, DVD, BluRay*, en discos virtuales que proporciona Internet o simplemente en otro Disco Duro, para posteriormente si pierde la información, poder restaurar el sistema.

Bluetooth: Es una tecnología de ondas de radio de corto alcance (2.4 GHz de frecuencia) cuyo objetivo es el simplificar las comunicaciones entre dispositivos informáticos, como ordenadores móviles, teléfonos móviles, otros dispositivos de mano y entre estos dispositivos e Internet. También pretende simplificar la sincronización de datos entre los dispositivos y otros ordenadores.

Bucaneros: Suelen ser personas sin ningún tipo de conocimientos, ni de electrónica, ni de informática, se tratan de comerciantes que se dedican a explotar lo que los Craker crean vendiendo los productos crackeados.

Caballos de Troya: Es un programa aparentemente útil que contiene funciones escondidas y además pueden explotar los privilegios de un usuario dando como resultado una amenaza hacia la seguridad. Un caballo de Troya es más peligroso que un administrador del sistema o un usuario con ciertos privilegios

Carding: Es el uso ilegitimo de las tarjetas de crédito, o de sus números, pertenecientes a otras personas. Donde para conseguir los números de tarjetas de créditos se basan en la utilización de Ingeniería Social.

Código de ética: Son sistemas de reglas establecidos con el propósito general de guiar el comportamiento de los integrantes de una organización y de aquellos con los cuales ésta actúa habitualmente: trabajadores, clientes, proveedores, contratistas, etc.

Computo forense: Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Confidencialidad: Servicio de seguridad o condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

Contrato electrónico: Es un acuerdo de voluntades, aunadas a través de redes digitales, destinadas a crear, modificar o transferir derechos de las partes.

Control de acceso: Un control de acceso se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que entonces le sea permitido el acceso.

Copyhackers: Estos personajes poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello "extraen" información del verdadero Hacker para terminar su trabajo. La principal motivación de estos nuevos personajes, es el dinero.

Copyright: Derecho que tiene un autor, incluido el autor de un programa informático, sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han ser éstas reproducidas y distribuidas. Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o tan generosa como el autor decida. El símbolo de este derecho es ©.

Crackers: Es una persona que mediante ingeniería inversa realiza: seriales, keygens y cracks, los cuales sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo.

Curiosos: Son personas que tienen un alta interés en las nuevas tecnologías, pero aún no tienen la experiencia ni conocimientos básicos para considerarlos hacker o crackers, generalmente no se trata de ataques dañinos, pero afecta el entorno de fiabilidad y confiabilidad generado en un sistema.

Delito informático: Es toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena. También los delitos informáticos se definen como "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".

Desastre: Se considera como un evento, frecuentemente concentrado en tiempo y espacio, en el cual la sociedad una parte de ella sufre severos daños, de gran magnitud y extensión, e incurre en pérdidas para sus miembros, de tal manera que su estructura social ya administrativa se desajusta, impidiendo la realización de sus actividades esenciales, afectando su funcionamiento y operación normales, perjudicando crucialmente su capacidad de afrontar y combatir la situación de emergencia.

Deontología informática: Trata de la moral o ética profesional en el manejo del activo más importante que tenemos, un bien cada vez más apreciado, *que es la información,* a través de los códigos de ética.

Disponibilidad: La disponibilidad es un servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información asociados en el lugar, momento y forma en que es requerido.

Enmascaramiento o engaño: Significa que se pretende ser alguien más, de tal manera que se puede obtener los derechos de acceso de una persona. El enmascaramiento envuelve un ataque en los controles de autenticación, por lo que el sistema puede enmascarse como otro sistema para engañar al usuario y descubrir información.

Estándar: Es una especificación que regula la realización de ciertos procesos o la fabricación de componentes para garantizar la interoperabilidad.

Ethernet: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus; tiene ancho de banda de 10 Mbps, por lo tanto tiene una elevada velocidad de transmisión y se ha convertido en un estándar de red.

Ética informática: Es la disciplina que analiza los problemas éticos que son creados por las tecnologías computacionales 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.

Ex-empleado: Definiéndolo de acuerdo al concepto del presente trabajo se refiere a personas descontentas con la organización y que conocen a la perfección la estructura del sistema, por consiguiente, tienen los conocimientos necesarios para causar cualquier tipo de daño.

Exploración: Consiste en el enviar una secuencia de información cambiante a una computadora para encontrar valores que muestren respuestas positivas, como son las contraseñas, números telefónicos, etc.

Firma electrónica: Es un conjunto de datos adjuntados o asociados a un mensaje y utilizados como medio para identificar al autor y garantizar la integridad de los documentos digitales.

Fraude: Cada año millones de dólares son sustraídos de las empresas y, en muchas ocasiones, las computadoras son utilizadas para dichos fines.

Gurús: Viene de una palabra del hindi que significaba "maestro, profesor", que a su vez procede de otra del sánscrito con el sentido de "poderoso". Po lo que se refiere a una persona a la que se le reconoce autoridad en alguna de las nuevas áreas tecnológicas suele recibir el nombre de gurú. Se refiere a una persona que se considera una eminencia en cierto tema, aunque no necesariamente tenga siempre la razón.

Gusanos: Los gusanos son programas que se propagan ellos mismos; un gusano hace una copia de sí mismo y lo realiza cuando es ejecutado. Los gusanos frecuentemente se propagan de una computadora a otra a través de las conexiones de la red. Los gusanos con frecuencia roban, destruyen o modifican datos en una computadora.

Hackers: Es aquella persona experta en el área de informática que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

Hipertexto: Es una tecnología que organiza una base de información en bloques distintos de contenidos, conectados a través de una serie de enlaces cuya activación o selección provoca la recuperación de información.

Hospedaje de sitios: Se refiere al lugar que ocupa una página web, sitio web, sistema, correo electrónico, archivos etc. En Internet o más específicamente en un servidor que por lo general hospeda varias aplicaciones o páginas web.

HTML: Siglas de **Hyper Text Markup Language** (*Lenguaje de Marcas de Hipertexto*), es el lenguaje predominante para la construcción de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes. HTML se escribe en forma de "etiquetas", rodeadas por corchetes angulares (<,>). HTML también puede describir, hasta un cierto punto, la apariencia de un documento, y puede incluir un script (por ejemplo Javascript), el cual puede afectar el comportamiento de navegadores web y otros procesadores de HTML.

HTTP (*HyperText Transfer Protocol o Protocolo de Transferencia de Hipertexto*): Es el protocolo usado para el intercambio de información en la Word Wide Web, es el método mediante el cual se transfieren las páginas web a una computadora.

Información: Es todo mensaje (conjunto de datos) que al receptor le interese, le entienda o lo ignore antes de recibirlo.

Informática: Es la información automatizada que es accedida a través de la tecnología asociada a la información, es decir, a través de medios automatizados.

Ingeniería social: es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan de forma que revelen datos indispensables que permitan superar las barreras de seguridad. Esta técnica es una de las más usadas y efectivas al momento de averiguar nombres de usuarios y contraseñas.

Ingeniería social inversa: Consiste en la generación, por parte de los intrusos, de una situación inversa a la original en la ingeniería social. En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios y éstos lo llaman ante algún

imprevisto. El intruso aprovechará esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el propio.

Integridad: Servicio de seguridad que garantiza que la información sea modificada, incluyendo su creación y borrado, sólo por el personal autorizado.

Interrupción: Es un ataque contra la disponibilidad, en el cual un recurso del sistema es destruido o se vuelve no disponible.

ISO: Es la **Organización Internacional de Normalización** o **ISO** es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

Intrusos remunerados: Se trata de crakers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar secretos o simplemente para dañar de alguna manera la imagen de la entidad atacada.

Lamers: Es una persona con falta de habilidades técnicas que se creen hackers pero hackean mediante programas creados por otras personas y se creen mejores que los usuarios promedio de computadoras solo por saber utilizar programas hechos por otros.

Lenguaje de programación: Es un conjunto de símbolos y reglas sintácticas que definen su estructura y el significado de sus elementos y expresiones, y es utilizado para controlar el comportamiento físico y lógico de una máquina.

Lenguaje de programación multiparadigma: Es el cual soporta más de un paradigma de programación y que permiten crear "programas usando más de un estilo de programación".

Lenguaje dinámico: Es todo aquel lenguaje que posea características que permitan alterar el curso del lenguaje de manera legítima, a través de la inyección de código o de la ejecución de funcionalidades especiales.

Lenguaje interpretado: Es un lenguaje de programación que necesita de un intérprete para la implementar o ejecutar el código escrito de éste.

Lenguaje multiplataforma: Es decir, pueden ejecutarse en cualquier plataforma Windows, Unix (Solaris, Silicon Graphics) y Power/Mac.

Manejador de base de datos: Es un módulo de programa que constituye la interfaz entre los datos de bajo nivel almacenados en la base de datos y los programas de aplicaciones y las consultas hechas al sistema.

Modificación: Es un amenaza que puede ocasionar grandes daños en el sistema debido a que una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo.

Newbie: Este término es utilizado para describir a un principiante de la computación, siendo comúnmente usado para indicar a usuarios de internet de prominente práctica pero de corto conocimiento técnico, a un recién llegado foro o comunidad.

No repudio: El no repudio previene a los emisores o a los receptores de negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

Perfil de Protección: Es un documento que se utiliza durante el proceso de evaluación de la norma CC, este documento define un conjunto de objetivos y requisitos de seguridad, independiente del entorno de implantación, para una categoría de productos de seguridad que cubre las necesidades de seguridad comunes a varios usuarios.

Phreakers: Son las personas con ciertos conocimientos y herramientas de hardware y software, que pueden engañar a las compañías telefónicas para que éstas no cobren las llamadas que se hacen.

Pixels: Un píxel o pixel (acrónimo del inglés picture element, "elemento de imagen") es la menor unidad homogénea en color que forma parte de una imagen digital, ya sea esta una fotografía, un fotograma de vídeo o un gráfico.

Plan de contingencias: Es una guía para la restauración rápida y organizada de las operaciones de cómputo después de una suspensión

Plataforma: Es un sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible.

Política de Seguridad: Conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.

Portal: Un **portal de Internet** es un sitio web cuya característica fundamental es la de servir de Puerta de entrada (única) para ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios relacionados a un mismo tema.

Privacidad: Conjunto de circunstancias, cosas, experiencias, sentimientos y conductas que un ser humano desea mantener reservado para sí mismo, con libertad de decidir a quién le da acceso

Programación Orientada a Objetos: Es un paradigma de la programación que usa objetos y sus interacciones, para diseñar aplicaciones y programas informáticos. Está basado en varias técnicas, incluyendo la herencia, abstracción, polimorfismo y encapsulamiento.

Propiedad Intelectual: Supone el reconocimiento de un derecho de propiedad especial en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano.

Protocolo: Es un conjunto de reglas usadas por la computadora para comunicarse unas con otras a través de una red.

Puerta trasera: Es el software contiene mecanismos escondidos que permiten a los diseñadores (o quienes sepan el secreto) desviar los controles.

Riesgo: La posibilidad de que un agente amenazador podrá atacar exitosamente en contra de una vulnerabilidad específica de un sistema.

Roll-backs: Es una operación que es utilizada en una base de datos, la cual permite a la base de datos algún estado previo después de realizar alguna operación.

Sabotaje: Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

Scriptkiddies: Son las personas que utilizan programas y scripts desarrollados por otros para atacar sistemas de computadoras y redes.

Seguridad: Característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible (es decir que el sistema se comporte tal y como se espera que funcione).

Seguridad informática: Es el conjunto de normas, mecanismos, herramientas, procedimientos y recursos orientados a brindar protección a la información resguardando sus disponibilidad, integridad y confidencialidad.

Servidor: Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

Servidor web: Es un servidor que almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.

Servlets: Es un objeto que se ejecuta en un servidor o contenedor JEE, especialmente diseñado para ofrecer contenido dinámico desde un servidor web, generalmente HTML.

Sitio web: Es una colección de páginas web relacionadas y comunes a un dominio de Internet o subdominio en la World Wide Web en Internet.

Sitio web estático: Son aquellos sitios enfocados principalmente a mostrar una información permanente, donde el navegante se limita a obtener dicha información, sin que pueda interactuar con la página Web visitada, las Web estáticas están construidas principalmente con hipervínculos o enlaces (links) entre las páginas Web que conforman el sitio, este tipo de Web son incapaces de soportar aplicaciones Web como gestores de bases de datos, foros, consultas on line, etc.

Sitio web dinámico: Son aquellos que permiten crear aplicaciones dentro de la propia Web, otorgando una mayor interactividad con el navegante. Aplicaciones dinámicas

como encuestas y votaciones, foros de soporte, libros de visita, envío de e-mails inteligentes, reserva de productos, pedidos on-line, atención al cliente personalizada.

Sniffing: Es un programa para monitorear y analizar el tráfico en una red de computadoras, detectando los cuellos de botellas y problemas que existan en ella.

Spoofing: Es el uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Tecnología de la información: Comprende todas las formas de tecnología empleadas para crear, almacenar, intercambiar y usar información en sus formas variadas (datos de negocios, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia y otras formas, incluyendo aquellas que aún no se han concebido). Es un término conveniente para incluir tanta a la telefonía como a la tecnología de cómputo en una misma palabra.

Terrorista: En esta definición se engloba a cualquier persona que ataca al sistema causando un daño de cualquier índole en él, tienen fines proselitistas o religiosos.

Trashing: Consiste en rastrear en las papeleras en busca de información, contraseñas o directorios.

Triggers: Es un procedimiento que se ejecuta cuando se cumple una condición establecida al realizar una operación.

Virus: Los virus son peligros porque se propagan ellos mismos e infectan a otras computadoras. Los virus pueden residir en discos o en cintas de respaldo y aparecen después de un largo tiempo de haber sido plantados o reaparecen después de mucho tiempo de ser supuestamente erradicados.

Vulnerabilidad: Son todas aquellas debilidades que se están presentando en el sistema, lo cual hace susceptible de ser afectado, alterado o destruido por alguna circunstancia indeseada, que afectan al funcionamiento normal o previsto de dicho sistema informático.

Webmaster: Es la persona responsable de mantenimiento o programación de un sitio web.

Wireless: Es la comunicación inalámbrica o sin cables en la que extremos de la comunicación (emisor/receptor) no se encuentran unidos por un medio de propagación físico, sino que se utiliza la modulación de ondas electromagnéticas a través del espacio.

INDICE DE FIGURAS

INDICE DE TABLAS

BIBLIOGRAFÍA

- Bravo Santos, C., & Redondo Duque, M. (2005). Sistemas nteractivos y colaborativos en la web. España: Ediciones de la Universidad de Castilla-La Mancha.

- Contreras Alarcón, J. (1997). INTERNET Telnet, FTP,Correo Electrónico,News,Gopher, World Wide Web. Madrid: PARANINFO.

- Daltabuit Godás, E., Hernández Audelo, L., Mallén Fullerton, G., & Vázquez Gómez, J. d. (2007). La seguridad de la información. México: Limusa.

- Eager, B. (1995). World Wide Web paso a paso. Estado de México: Prentice-Hall Hisponoamericana.

- Ferreyra Cortés , G. (1995). VIRUS EN LAS COMPUTADORAS. México, D.F: Alfaomega Grupo Editor, S.A, de C.v.

- Ferreyra Cortés, G. (1996). Internet paso a paso. Hacia la autopista de la información. México: Alfaomega Grupo Editor, S.A de C.V.

- Firtman, M. R. (2010). AJAX Web2.0 con jQuery para profesionales (2 ed.). México DF: Alfaomega.

- Fumero, A., Roca, G., & Sáez Vacas, F. (2007). Web 2.0. España: Fundación Orange, Creative Commons.

- Gratton, P. (1998). Protección Informática en datos, en gestion, en equipos y redes en internet. México: trillas.

- John Wecker y Douglas Adeney, Ética Informática y de las Ciencias de la Información, 1ra. Edición, editorial Fragua, Madrid 2000.
- Kevin W. Browyer, Ethics And Computing Living Responsibly In a Computerized World, 2da edición, editorial IEEE PRESS, New York U.S.A 2001.

- Labodía Bonastre, J. A. (1994). Protección de activos informáticos. Madrid: Fundacion MAPFRE.

- López Barrientos, M. J., & Quezada Reyes, C. (2006). Fundamentos de Seguridad Informática. México: UNAM, Facultad de Ingeniería.

- Orós, J. (2007). Diseño de páginas Wen con XHTML, JavaScript y CSS. México: Alfaomega.

- Randall, N. (1994). Aprendiendo Internet en 21 días. México: PRENTICE HALL HISPANOAMERICANA , S.A.

- Siyan, K., & Hare, C. (1997). Fire Walls y la Seguridad en Internet. México: Prentice-Hall Hispanoamericana, S.A.

- Stallings, William, Fundamentos de seguridad: aplicaciones y estnadares, 2da, edición, Editorial Person Education, Madrid 2004.

- Suehring, S., Converse, T., & Park, J. (2009). PHP 6 Y MySQL. Madrid: ANAYA.

- Walker, Andy. (2006). Manual Imprescindible de Seguridad, sapm, spyware y virus. Madrid: GRUPO ANAYA, S.A.

REFERENCIAS WEB

Seguridad de aplicaciones Web ASP.NET

http://msdn.microsoft.com/es-es/library/330a99hc(VS.80).aspx

Vulnerabilidad que afecta a las versiones anteriores a Ruby 1.8.X

http://www.websecurity.es/?q=vulnerabilidad-que-afecta-las-versiones-anteriores-ruby-1-8-

Las 75 Herramientas de Seguridad Más Usadas

http://insecure.org/tools/tools-es.html

Herramientas de seguridad:

http://www.acunetix.com/

http://www.aircrack-ng.org/

http://airsnort.shmoo.com/

http://www.angryip.org/w/Home

http://www.securityfocus.com/tools/142

http://bastille-linux.sourceforge.net/

http://portswigger.net/burp/

http://www.oxid.it/cain.html

http://www.nessus.org/products/nessus

http://www.ethereal.com/

http://www.snort.org/

http://www.symantec.com/business/index.jsp

http://www.tcpdump.org/

http://www.hping.org/

http://www.gfi.com/network-security-vulnerability-scanner/

http://ettercap.sourceforge.net/

http://www.openwall.com/john/

http://www.openssh.com/

http://www-935.ibm.com/services/us/en/it-services/gts-it-service-home-page-1.html

http://www.tripwire.com/

http://www.cirt.net/nikto2

http://www.kismetwireless.net/

http://www.eeye.com/products

http://www.saintcorporation.com/index.html

http://www-arc.com/sara/

http://www.gnupg.org/

http://www.oxid.it/cain.html

http://www.openssl.org/

http://www.hoobie.net/brutus/

http://www.stunnel.org/

http://www.monkey.org/~dugsong/fragroute/

Código penal federal

http://info4.juridicas.unam.mx/ijure/tcfed/8.htm

Derechos de autor

http://info4.juridicas.unam.mx/ijure/fed/153/default.htm?s

Protección de datos personales para el DF

http://iibi.unam.mx/archivistica/ley_datos_personales_df.pdf