AUDITORÍA DE SISTEMAS

INFORMÁTICOS

ISBN: 978-9942-14-042-5
Título: Auditoría de Sistemas Informáticos
Autor: Quintanilla Romero, Marco Antonio
De La Torre Lascano, Carlos Mauricio
Editorial: MQR®

Materia: Educación. investigación. temas relacionados con la tecnología
Publicado: 2012-01-22
NºEdición: 2
Idioma: Español

www.uceinvestigar.com

AUDITORÍA DE SISTEMAS INFORMÁTICOS

ÍNDICE

LISTA DE FIGURAS

INTRODUCCION

Los Sistemas Informáticos se han constituido en la columna vertebral de toda organización, con estos sistemas se pueden realizar desde operaciones muy sencillas, hasta operación que procesan información y contribuyen a tomar decisiones en las empresas.

Las Tecnologías de la Información TIC'S, están inmersa en la gestión integral de la empresa. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado la gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la auditoria Informática.

El término de Auditoria se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. A causa de esto, se ha tomado la frase "Tiene Auditoria" como sinónimo de que, en dicha entidad, antes de realizarse la auditoria, ya se habían detectado fallas.

La palabra auditoria proviene del latín "auditorius", y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír.

La auditoría es un examen, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

El auditor informático ha de velar por la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz sistema de información.

Claro está, que para la realización de una auditoria informática eficaz, se debe entender a la empresa en su más amplio sentido, ya que una universidad, un ministerio o un hospital son tan empresas como una sociedad anónima o empresa Pública, al igual que en este caso, un Centro de Comunicaciones, no importa al sector al cual pertenezca el ente que va a ser auditado sea público o privado, ambos utilizan la informática para gestionar sus negocios de forma rápida y eficiente, con el fin de obtener beneficios económicos y reducción de costos.

Por eso, al igual que los demás órganos de la empresa (Balances y Cuentas, Tarifas, Sueldos, etc.), los Sistemas Informáticos están sometidos al control correspondiente, o al menos debería estarlo.

CAPÍTULO I

1. AUDITORÍA DE SISTEMAS ESPECIALIZADA I

Evalúa normas, controles, técnicas y procedimientos establecidos en una empresa para lograr confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de los sistemas de información. Es una rama de la auditoría, que se especializa en promover y aplicar conceptos de auditoría en el área de sistemas de información.

Verifica controles en el procesamiento de la información, desarrolla e instala sistemas; su objetivo es evaluar la efectividad y direccionar a la gerencia.

1.1. OBJETIVOS

- Comprender la evaluación de los procesos del Área de Procesamiento automático de Datos (PAD) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas.
- Comprende el proceso de recolección y evaluación de evidencia para determinar si un sistema esta automatizado:

Figura No. 1: Proceso de recolección y evaluación

La auditoría de sistemas como rama especializada de la auditoría promueve y aplica conceptos de la misma, en el área de tecnología de la información (TI).

Figura No. 2: Auditoria de Sistemas

1.2. IMPORTANCIA

Es importante porque través de su sistematización organizacional, evalúa la función de tecnología de información y brinda su aporte para el cumplimiento de los objetivos institucionales, emitiendo opiniones y recomendaciones para mejorar el cumplimiento de dichos objetivos.

Figura No. 3: Procesamiento de datos

Examina y evalúa procesos del área de Procesamiento Automático de Datos (PAD) y de la utilización de los recursos económicos de los sistemas computarizados en una organización, para posteriormente presentar conclusiones y recomendaciones a la gerencia con el propósito de corregir las deficiencias existentes y mejorarlas.

1.3. FINALIDAD

- Participar en la planeación del trabajo de auditoría, identificando los riesgos y controles principalmente.
- Colaborar con el cumplimiento de los procesos de planeación, desarrollo, mantenimiento y operación de los sistemas de procesamiento por sistemas computarizados.
- Fundamentar la opinión del auditor interno (externo) respecto a la confiabilidad de los sistemas de información
- Expresar una opinión referente a la eficiencia de las operaciones en el área de TI.

1.3.1. Apoyo de la Auditoría interna

A pesar de constituir una función de evaluación independiente, existe en una entidad, bajo la autorización de la dirección con el objeto de examinar y evaluar las actividades de la entidad. La principal función que cumple el auditor interno consiste en ayudar a la dirección en la realización de sus funciones, asegurando:

- Salvaguardia del inmovilizado material e inmaterial de la entidad.
- Exactitud y fiabilidad de los registros contables.
- Fomento de la eficiencia operativa
- Adhesión a las políticas de la entidad y el cumplimiento de sus obligaciones legales.

El auditor interno, siempre se ocupa de la adecuación a los controles sobre las actividades mecanizadas, al igual que lo hace con la eficiencia y eficacia de los procedimientos empleados en el manejo de los costos.

1.3.2. Apoyo de la Auditoría externa

Constituye una función de evaluación independiente y externa a la entidad que se examina. Las empresas, en su mayoría, contratan anualmente la realización de una auditoría de los estados financieros, por parte de un contador público independiente, sea voluntariamente o por una obligación legal.

El objetivo principal de una auditoría externa es la expresión de una opinión respecto de la calidad de los estados financieros de la entidad, por lo que el auditor externo se ocupa principalmente de la fiabilidad de la información financiera.

1.3.3. Diferencia entre Auditoría Interna y Externa

La auditoría interna se lleva a cabo con personas perteneciente a la misma organización, la externa exige como condición de credibilidad, que los profesionales que la realizan no formen parte de la empresa auditada, deben ser independientes a ella y a sus directivos.

Las auditorías externas se desarrollan bajo parámetros estandarizados que no pueden ser substancialmente alterados ni modificados, los procedimientos de auditoría interna son más flexibles y dependen más de la empresa, sus dirigentes o de los responsables de auditoría interna

1.3.4. Auditoría Interna y sus Relaciones

Figura No. 4: Auditoria y sus relaciones

a) Dentro de la empresa	b) Con la auditoría externa
• Profesionalidad discreción. • Auditoría interna debe ser entendida como un colaborador/asesor que indique la mejor manera de hacer las cosas, apunte las deficiencias para que sean corregidas por los auditados y que escuche aspiraciones, sugerencias o innovaciones • Debe tener un conocimiento real de las funciones que cada unidad lleva a cabo, familiarizarse con ellas y formar equipos con trabajadores para documentarse, previo a la realización de programas concretos de auditoría de gestión.	• Un departamento de auditoría interna exige tener buenas relaciones con los auditores externos. • Las normas y prácticas de auditoría establecen muy claramente necesidades de una actuación coordinada y eficaz de ambos auditores, es necesario evitar afectos perturbadores en las relaciones con los auditores externos como consecuencia de los requisitos de trabajo complementario que estos hacen a los auditores internos.

1.3.5. Aspecto del medio ambiente informático que afecta el enfoque de la Auditoría y sus procedimientos

Figura No. 5: Medio ambiente informático

1.3.6. Razones para la existencia de la función de la Auditoría de Sistemas

La información es un recurso clave en las empresas, sus utilidades son importantes para:

- Planear el futuro, controlar el presente y evaluar el pasado organizacional.
- Las operaciones organizacionales dependientes cada vez más de la sistematización.

Los riesgos tienden aumentar, debido a:

- Perdida de información
- Pérdida de activos
- Pérdida de servicios, ventas

La sistematización representa un costo significativo para la empresa en cuanto a:

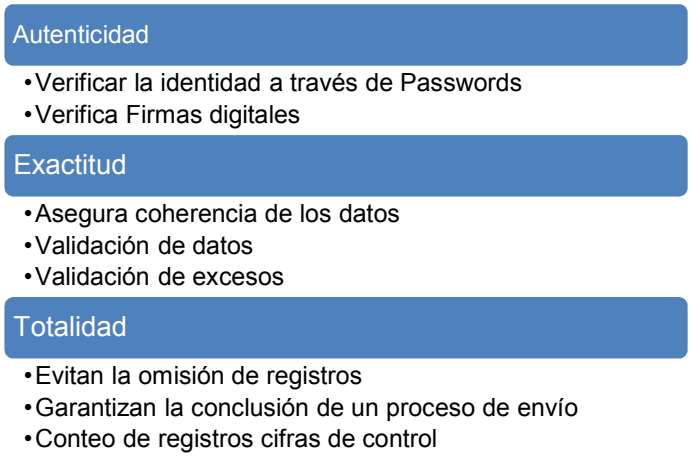
- Hardware, software y personal.
- Los problemas se identifican sólo al final
- El permanente avance tecnológico.

1.3.7. Requerimiento del Auditor de Sistemas

- Entendimiento global e integral del negocio y la empresa, puntos claves, áreas críticas, entorno económico, social y político.
- Entendimiento del efecto de los sistemas en la organización
- Entendimiento de los objetivos de auditoría
- Conocimientos de los recursos de computación de la empresa
- Conocimiento de los proyectos de sistemas

1.3.8. Principales Controles físicos y lógicos de auditorías

Figura No. 6: Controles



1.3.9. Ponentes Auditables

- Plataformas
- Sistemas Aplicativos
- Procesos Automatizados

1.4. COMPONENTES BÁSICOS DE UN SISTEMA DE COMPUTACIÓN

Las computadoras se han vuelto una herramienta esencial, en casi todos los campos de nuestra vida cotidiana; es de gran utilidad y ayuda a la mejora y excelencia del trabajo; haciéndolo más fácil y práctico. Las computadoras han transformado los procesos laborales complejos y de gran dificultad hacia una manera más eficiente en la resolución de problemas difíciles, buscando una solución práctica.

Los dispositivos periféricos de la computadora juegan un papel esencial, volviéndola más útil a los usuarios. Estos dispositivos ayudan a introducir datos que optimizan y resuelven problemas y operaciones de manera digital y ya no de forma manual. La computadora necesita de entradas para poder generar salidas y éstas se dan a través de dos tipos de dispositivos periféricos:

1.4.1. Dispositivos Periféricos de Entrada.

Estos dispositivos permiten al usuario del computador introducir datos, comandos y programas en el CPU. Los datos se leen de los dispositivos de entrada y se almacenan en la memoria central o interna, estos dispositivos, convierten la información en señales eléctricas que se almacenan en la memoria central. Entre el periférico de salida, estos son las más conocidos:

Figura No. 7: Dispositivos de entrada

Teclado		dispositivo eficaz para introducir datos no gráficos como rótulos de imágenes asociados con un despliegue de gráficas
Mouse o ratón		Da instrucciones a nuestra computadora a través de un cursor que aparece en la pantalla y haciendo clic para que se lleve a cabo una acción determinada; es el elemento periférico que más se utiliza en una PC.
Micrófono		Son traductores encargados de transformar energía acústica en energía eléctrica, permitiendo, por lo tanto el registro, almacenamiento, transmisión y procesamiento electrónico de las señales de audio. Son dispositivos duales de los altoparlantes, constituye.
Scanner		Permite la introducción de imágenes gráficas al computador mediante un sistema de matrices de puntos, como resultado de un barrido óptico del documento.

Cámara Digital		Se conecta al ordenador y le transmite las imágenes que capta, pudiendo ser modificada y retocada, o volverla a tomar en caso de que este mal
Cámara de Video		Graba videos en formato digital, que es mucho mejor la imagen, tiene una pantalla LCD por la que ves simultáneamente la imagen mientras grabas. Se conecta al PC y este recoge el video que has grabado, para poder retocarlo posteriormente con el software adecuado
Webcam		Cámara de pequeñas dimensiones, está conectada al PC para poder funcionar. Se utiliza para videoconferencias por Internet, se pueden grabar videos como una cámara normal y tomar fotos estáticas; entre otras.

Permiten al usuario ver los resultados de los cálculos o de las manipulaciones de datos de la computadora. El dispositivo de salida más común es la unidad de visualización (VDU, acrónimo de Video Display Unit), que consiste en un monitor que presenta los caracteres y gráficos en una pantalla similar a la del televisor.

Los tipos de dispositivos de salida más comunes son:

Figura No. 8: Dispositivos de Salidad

Pantalla o Monitor		Es un aparato basado en un tubo de rayos catódicos (CRT) como el de los televisores, mientras que en los portátiles es una pantalla plana de cristal líquido (LCD). Es en donde se visualiza la información suministrada por el ordenador.
Impresora		Es el periférico que el ordenador utiliza para reproducir la información en forma tangible, es decir se encarga de imprimir la información.
Altavoces o parlantes		Dispositivos por los que se emiten sonidos procedentes de la tarjeta de sonido. Existen en la actualidad diversos ejemplares que cubren la oferta del mercado.

Auriculares		Son dispositivos que se colocan en el oído, para escuchar los sonidos que la tarjeta de sonido envía. Presentan la ventaja de que no pueden ser escuchados por otra persona, solo la que los utiliza.
Plotters		Son trazadores de gráficos a escalas superiores que una impresora normal, empleado generalmente para trabajos de diseño, arquitectura, ingeniería civil y topografía
Fax		Dispositivo mediante el cual se imprime una copia de otro impreso, transmitido, vía teléfono, o desde el propio fax.

1.4.2. Dispositivo de Almacenamiento

Figura No. 9: Dispositivos de Almacenamiento

Unidades de cinta magnética		Por varios años las cintas magnéticas fueron el único tipo de almacenamiento no volátil disponible. El almacenamiento secuencial en una cinta requiere que la unidad de cinta magnética lea estas desde el principio hasta llegar al archivo de datos deseado.
Unidades de disquetes		El disquete o disco flexible es un soporte de almacenamiento de datos de tipo magnético, formado por una fina lámina circular de material magnetizable y flexible, se utilizaba en la computadora, para disco de arranque, para trasladar datos e información de una computadora a otra, o simplemente para almacenar y resguardar archivos.
Discos duros		Los sistemas de discos duros son muy importantes como medios de almacenamiento en los sistemas computacionales, ya que pueden almacenar datos en mayor cantidad y más rápidamente, igualmente su recuperación es más rápida que en los disquetes.

Discos ópticos		Es un medio de almacenamiento de datos, consiste en un disco circular en el cual la información se codifica, guarda y almacena, mediante surcos microscópicos hechos con un láser, se puede guardar cualquier tipo o morfología de información (texto, imagen, audio, vídeo, etc.) Aunque no son tan rápidos como los discos duros, los discos ópticos tienen mucho espacio para almacenar datos y son menos sensibles a las fluctuaciones ambientales.
Memoria Flash		Es un tipo de memoria que se comercializa para el uso de aparatos portátiles, como cámaras digitales o agendas electrónicas. El aparato correspondiente o bien un lector de tarjetas, se conecta a la computadora a través del puerto USB o Firewire.
Tarjeta de memoria		Una tarjeta de memoria es un pequeño soporte de almacenamiento que utiliza memoria USB para guardar la información que puede requerir o no baterías. Estas memorias son resistentes a factores ambientales como el polvo.

1.4.3. Diferencia entre los dispositivos de E/S y almacenamiento de un computador

Los dispositivos de entrada son aquellos que permiten la comunicación entre la computadora y el usuario, son aquellos en donde la información ingresa desde el exterior hacia el interior del computador, convierten la información en señales eléctricas que se almacenan en la memoria central.

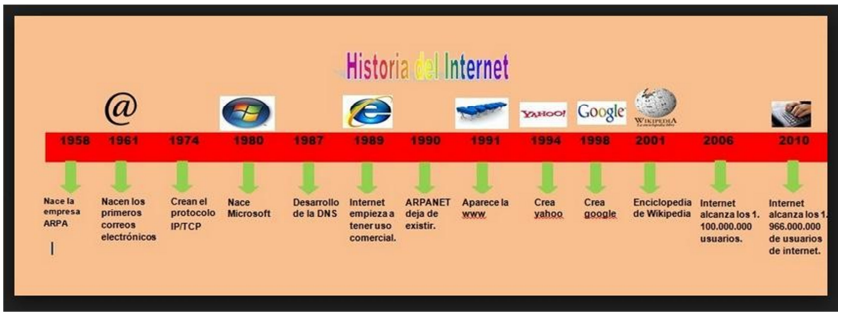
Mientras que los dispositivos de salida son todos aquellos elementos, los cuales nos permiten ver o distinguir la respuesta; son aquellos en donde la información sale desde el interior del computador hacia el exterior y por último, los dispositivos de almacenamiento son todo aparato que se utilice para grabar los datos de la computadora en forma permanente o temporal.

1.5. El INTERNET

Internet se inició como un proyecto de defensa de los Estados Unidos. A finales de los años 60, la ARPA (Agencia de Proyectos de Investigación Avanzados) del Departamento de Defensa definió el protocolo TCP/IP. Nace con la idea de garantizar la comunicación mediante este

sistema, entre lugares alejados en caso de ataque nuclear. Ahora el TCP/IP sirve para garantizar la transmisión de los paquetes de información entre lugares remotos, siguiendo cualquier ruta disponible.

Figura No. 10: Internet



En 1975, ARPAnet comenzó a funcionar como red, sirviendo como base para unir centros de investigación militares y universidades, y se trabajó en desarrollar protocolos más avanzados para diferentes tipos de ordenadores y cuestiones específicas. En 1983 se adoptó el TCP/IP como estándar principal para todas las comunicaciones, y en 1990 desapareció ARPAnet para dar paso junto a otras redes TCP/IP a Internet. Por aquel entonces también comenzaron a operar organizaciones privadas en la Red.

Poco a poco, todos los fabricantes de ordenadores personales y redes han incorporado el TCP/IP a sus sistemas operativos, de modo que en la actualidad cualquier equipo está listo para conectarse a Internet. Internet une muchas redes, incluyendo como más importantes la que proporciona acceso a los grupos de noticias (Usenet), que data de 1979 y (conceptualmente) la World Wide Web, de principios de los 90.

Se calcula que actualmente hay varios miles de redes de todos los tamaños conectadas a Internet, más de seis millones de servidores y entre 40 y 50 millones de personas que tienen acceso a sus contenidos. Y estas cifras crecen sin cesar de un día a otro.

1.5.1. Orígenes delInternet

La primera descripción documentada acerca de las interacciones sociales que podrían ser propiciadas a través del networking (trabajo en red) está contenida en una serie de memorándums escritos por J.C.R. Licklider, del Massachusetts Institute of Technology, en Agosto de 1962, en los cuales Licklider discute sobre su concepto de Galactic Network (Red Galáctica).

Licklider concibió una red interconectada globalmente a través de la que cada uno pudiera acceder desde cualquier lugar a datos y programas. En esencia, el concepto era muy parecido a la Internet actual. Licklider fue el principal responsable del programa de investigación en ordenadores de la DARPA desde Octubre de 1962. Mientras trabajó en DARPA convenció a sus sucesores Ivan Sutherland, Bob Taylor, y el investigador del MIT Lawrence G. Roberts de la importancia del concepto de trabajo en red.

En Julio de 1961 Leonard Kleinrock publicó desde el MIT el primer documento sobre la teoría de conmutación de paquetes. Kleinrock convenció a Roberts de la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red. El otro paso fundamental fue hacer dialogar a los ordenadores entre sí.

Para explorar este terreno, en 1965, Roberts conectó un ordenador TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera aunque reducida red de ordenadores de área amplia jamás construida. El resultado del experimento fue la constatación de que los ordenadores de tiempo compartido podían trabajar juntos correctamente, ejecutando programas y recuperando datos a discreción en la máquina remota, pero que el sistema telefónico de conmutación de circuitos era totalmente inadecuado para esta labor. La convicción de Kleinrock acerca de la necesidad de la conmutación de paquetes quedó pues confirmada.

A finales de 1966 Roberts se trasladó a la DARPA a desarrollar el concepto de red de ordenadores y rápidamente confeccionó su plan para ARPANET, publicándolo en 1967. En la conferencia en la que presentó el documento se exponía también un trabajo sobre el concepto de red de paquetes a cargo de Donald Davies y Roger Scantlebury del NPL. Scantlebury le habló a Roberts sobre su trabajo en el NPL así como sobre el de Paul Baran y otros en RAND. El grupo RAND había escrito un documento sobre redes de conmutación de paquetes para comunicación vocal segura en el ámbito militar, en 1964.

Ocurrió que los trabajos del MIT (1961-67), RAND (1962-65) y NPL (1964-67) habían discurrido en paralelo sin que los investigadores hubieran conocido el trabajo de los demás. La palabra packet (paquete) fue adoptada a partir del trabajo del NPL y la velocidad de la línea propuesta para ser usada en el diseño de ARPANET fue aumentada desde 2,4 Kbps hasta 50 Kbps.

En Agosto de 1968, después de que Roberts y la comunidad de la DARPA hubieran refinado la

estructura global y las especificaciones de ARPANET, DARPA lanzó un RFQ para el desarrollo de uno de sus componentes clave: los conmutadores de paquetes llamados interface message processors (IMPs, procesadores de mensajes de interfaz).

El RFQ fue ganado en Diciembre de 1968 por un grupo encabezado por Frank Heart, de Bolt Beranek y Newman (BBN). Así como el equipo de BBN trabajó en IMPs con Bob Kahn tomando un papel principal en el diseño de la arquitectura de la ARPANET global, la topología de red y el aspecto económico fueron diseñados y optimizados por Roberts trabajando con Howard Frank y su equipo en la Network Analysis Corporation, y el sistema de medida de la red fue preparado por el equipo de Kleinrock de la Universidad de California, en Los Angeles (6). A causa del temprano desarrollo de la teoría de conmutación de paquetes de Kleinrock y su énfasis en el análisis, diseño y medición, su Network

Measurement Center (Centro de Medidas de Red) en la UCLA fue seleccionado para ser el primer nodo de ARPANET. Todo ello ocurrió en Septiembre de 1969, cuando BBN instaló el primer IMP en la UCLA y quedó conectado el primer ordenador host.

El proyecto de Doug Engelbart denominado Augmentation of Human Intelect (Aumento del Intelecto Humano) que incluía NLS, un primitivo sistema hipertexto, el Instituto de Investigación de Standford (SRI) proporcionó un segundo nodo. El SRI patrocinó el Network Information Center, liderado por Elizabeth (Jake) Feinler, que desarrolló funciones tales como mantener tablas de nombres de host para la traducción de direcciones así como un directorio de RFCs (Request For Comments).

Un mes más tarde, cuando el SRI fue conectado a ARPANET, el primer mensaje de host a host fue enviado desde el laboratorio de Leinrock al SRI. Se añadieron dos nodos en la Universidad de California, Santa Bárbara, y en la Universidad de Utah. Estos dos últimos nodos incorporaron proyectos de visualización de aplicaciones, con Glen Culler y Burton Fried en la UCSB investigando métodos para mostrar funcionesmatemáticas mediante el uso de "storage displays" (**N. del T.** : mecanismos que incorporan buffers de monitorización distribuidos en red para facilitar el refresco de la visualización) para tratar con el problema de refrescar sobre la red, y Robert Taylor y Ivan Sutherland en Utah investigando métodos de representación en 3-D a través de la red.

Así, a finales de 1969, cuatro ordenadores host fueron conectados cojuntamente a la ARPANET inicial y se hizo realidad una embrionaria Internet. Incluso en esta primitiva etapa, hay que reseñar que la investigación incorporó tanto el trabajo mediante la red ya existente como la

mejora de la utilización de dicha red. Esta tradición continúa hasta el día de hoy.

Se siguieron conectando ordenadores rápidamente a la ARPANET durante los años siguientes y el trabajo continuó para completar un protocolo host a host funcionalmente completo, así como software adicional de red. En Diciembre de 1970, el Network Working Group (NWG) liderado por S.Crocker acabó el protocolo host a host inicial para ARPANET, llamado Network Control Protocol (NCP, protocolo de control de red). Cuando en los nodos de ARPANET se completó la implementación del NCP durante el periodo 1971-72, los usuarios de la red pudieron finalmente comenzar a desarrollar aplicaciones.

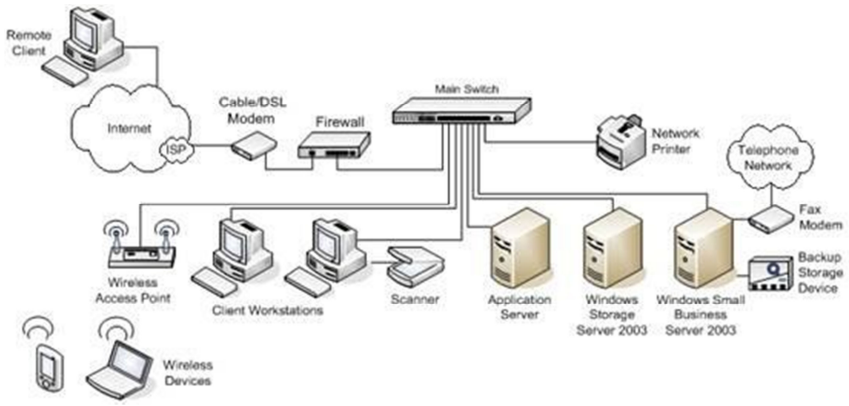
En Octubre de 1972, Kahn organizó una gran y muy exitosa demostración de ARPANET en la International Computer Communication Conference. Esta fue la primera demostración pública de la nueva tecnología de red. Fue también en 1972 cuando se introdujo la primera aplicación "estrella": el correo electrónico. En Marzo, Ray Tomlinson, de BBN, escribió el software básico de envío- recepción de mensajes de correo electrónico, impulsado por la necesidad que tenían los desarrolladores de ARPANET de un mecanismo sencillo de coordinación.

En Julio, Roberts expandió su valor añadido escribiendo el primer programa de utilidad de correo electrónico para relacionar, leer selectivamente, almacenar, reenviar y responder a mensajes. Desde entonces, la aplicación de correo electrónico se convirtió en la mayor de la red durante más de una década. Fue precursora del tipo de actividad que observamos hoy día en la World Wide Web, es decir, del enorme crecimiento de todas las formas de tráfico persona a persona.

1.5.1. La Red.

Internet es un conjunto de redes, redes de ordenadores y equipos físicamente unidos mediante cables que conectan puntos de todo el mundo. Estos cables se presentan en muchas formas: desde cables de red local (varias máquinas conectadas en una oficina o campus) a cables telefónicos convencionales, digitales y canales de fibra óptica que forman las "carreteras" principales. Esta gigantesca Red se difumina en ocasiones porque los datos pueden transmitirse vía satélite, o a través de servicios como la telefonía celular, o porque a veces no se sabe muy bien a dónde está conectada.

Figura No. 11: La Red



En cierto modo, no hay mucha diferencia entre Internet y la red telefónica que todos conocemos, dado que sus fundamentos son parecidos. Basta saber que cualquier cosa a la que se pueda acceder a través de algún tipo de "conexión," como un ordenador personal, una base de datos en una universidad, un servicio electrónico de pago (como CompuServe), un fax o un número de teléfono, pueden ser, y de hecho forman, parte de Internet.

El acceso a los diferentes ordenadores y equipos que están conectados a Internet puede ser público o estar limitado. Una red de cajeros automáticos o terminales de banco, por ejemplo, pueden estar integradas en Internet pero no ser de acceso público, aunque formen parte teórica de la Red. Lo interesante es que cada vez más de estos recursos están disponibles a través de Internet: fax, teléfono, radio, televisión, imágenes de satélites o cámaras de tráfico son algunos ejemplos.

En cuanto a organización, Internet no tiene en realidad una cabeza central, ni un único organismo que la regule o a la que pedirle cuentas si funciona mal. Gran parte de la infraestructura es pública, de los gobiernos mundiales, organismos y universidades. Muchos grupos de trabajo trabajan para que funcione correctamente y continúe evolucionando. Otra gran parte de Internet es privada, y la gestionan empresas de servicios de Internet (que dan acceso) o simplemente publican contenidos.

Como Internet está formada por muchas redes independientes, que hablan el mismo lenguaje, ni siquiera están claros sus límites.

1.5.2. Redes Globales

Es un conjunto de dispositivos físicos "hardware" y de programas "software", mediante el cual

podemos comunicar computadoras para compartir recursos (discos, impresoras, programas, etc.) así como trabajo (tiempo de cálculo, procesamiento de datos, etc.).

A cada una de las computadoras conectadas a la red se le denomina un nodo. Se considera que una red es local si solo alcanza unos pocos kilómetros.

1.5.2. Tipos de Redes

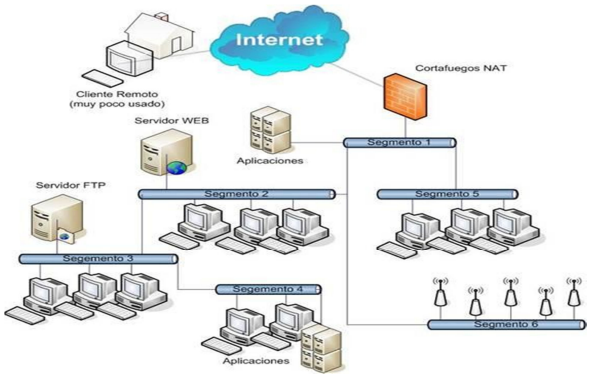
Las redes de información se pueden clasificar según su extensión y su topología. Una red puede empezar siendo pequeña para crecer junto con la organización o institución. A continuación se presenta los distintos tipos de redes disponibles:

Extensión de acuerdo con la distribución geográfica:

- **Segmento de red (subred)**

Un segmento de red suele ser definido por el "hardware" o una dirección de red específica. Por ejemplo, en el entorno "Novell NetWare", en un segmento de red se incluyen todas las estaciones de trabajo conectadas a una tarjeta de interfaz de red de un servidor y cada segmento tiene su propia dirección de red.

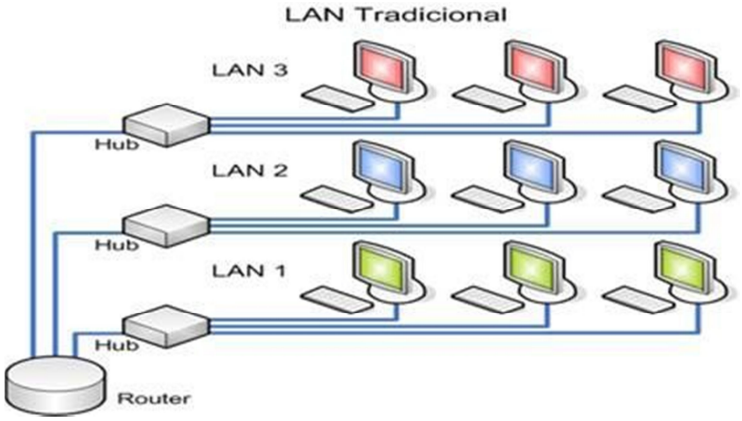
Figura No. 12: Segmento de Red



- **Red de área locales (LAN)**

Una LAN es un segmento de red que tiene conectadas estaciones de trabajo y servidores o un conjunto de segmentos de red interconectados, generalmente dentro de la misma zona. Por ejemplo un edificio.

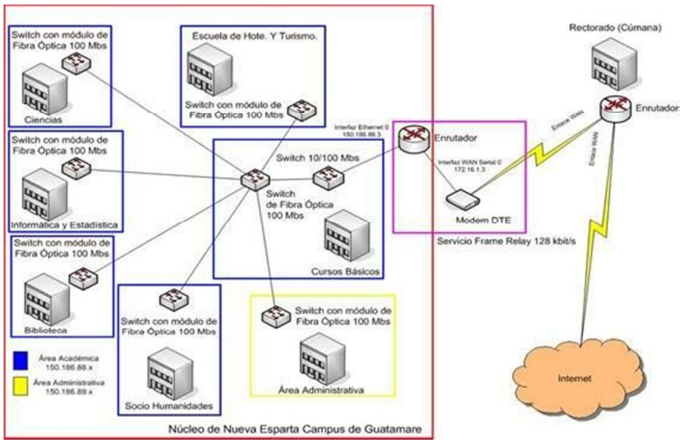
Figura No. 13: Red de áreas locales LAN



- **Red de campus**

Una red de campus se extiende a otros edificios dentro de un campus o área industrial. Los diversos segmentos o LAN de cada edificio suelen conectarse mediante cables de la red de soporte.

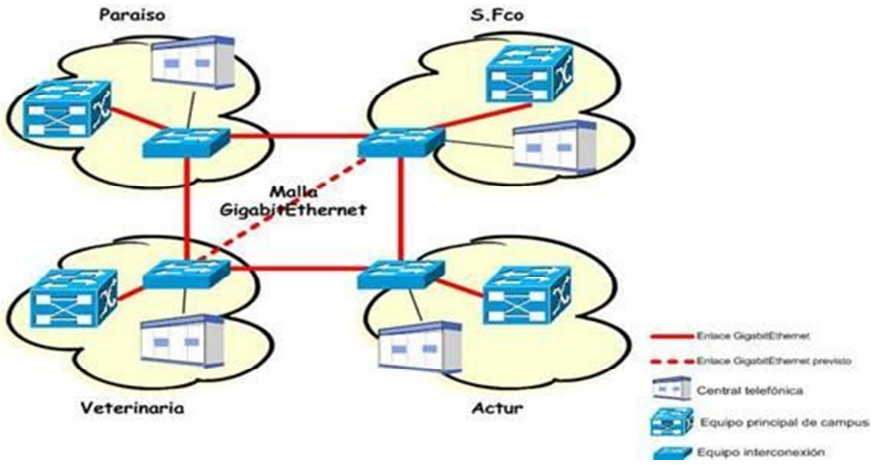
Figura No. 13: Red de campus



- **Red de áreas metropolitanas (MAN)**

Una red MAN es una red que se expande por pueblos o ciudades y se interconecta mediante diversas instalaciones públicas o privadas, como el sistema telefónico o los suplidores de sistemas de comunicación por microondas o medios ópticos.

Figura No. 14: Redes de área MAN



- **Red de área extensa (WAN y redes globales)**

Las WAN y redes globales se extienden sobrepasando las fronteras de las ciudades, pueblos o naciones. Los enlaces se realizan con instalaciones de telecomunicaciones públicas y privadas, además por microondas y satélites.

Figura No. 15: Redes WAN y LAN

1.5.3. Como funciona Internet

En Internet, las comunicaciones concretas se establecen entre dos puntos: uno es el ordenador personal desde el que usted accede y el otro es cualquiera de los servidores que hay en la Red y facilitan información.

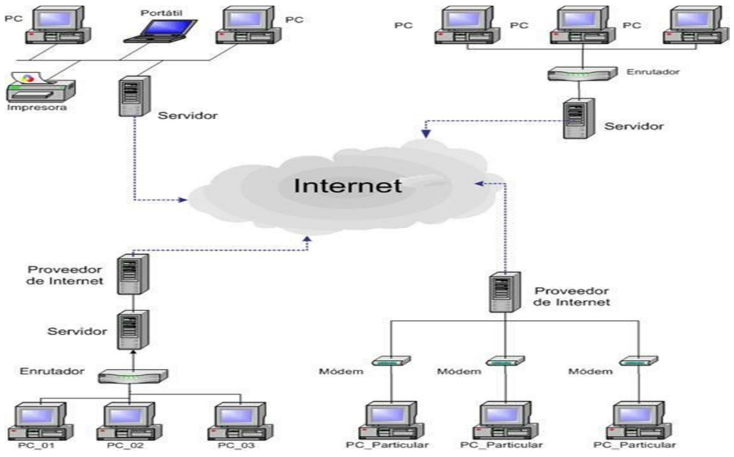
El fundamento de Internet es el TCP/IP, un protocolo de transmisión que asigna a cada máquina que se conecta un número específico, llamado "número IP" (que actúa a modo de "número

teléfono único") como por ejemplo 192.555.26.11.

El protocolo TCP/IP sirve para establecer una comunicación entre dos puntos remotos mediante el envío de información en paquetes. Al transmitir un mensaje o una página con imágenes, por ejemplo, el bloque completo de datos se divide en pequeños bloques que viajan de un punto a otro de la red, entre dos números IP determinados, siguiendo cualquiera de las posibles rutas. La información viaja por muchos ordenadores intermedios a modo de repetidores hasta alcanzar su destino, lugar en el que todos los paquetes se reúnen, reordenan y convierten en la información original. Millones de comunicaciones se establecen entre puntos distintos cada día, pasando por cientos de ordenadores intermedios.

La gran ventaja del TCP/IP es que es inteligente. Como cada intercambio de datos está marcado con números IP determinados, las comunicaciones no tienen por qué cruzarse. Y si los paquetes no encuentran una ruta directa, los ordenadores intermedios prueban vías alternativas. Se realizan comprobaciones en cada bloque para que la información llegue intacta, y en caso de que se pierda alguno, el protocolo lo solicita de nuevo hasta que se obtiene la información completa.

Figura No. 16: Funcionamiento Internet



TCP/IP es la base de todas las máquinas y software sobre el que funciona Internet: los programas de correo electrónico, transferencia de archivos y transmisión de páginas con texto e imágenes y enlaces de hipertexto. Cuando es necesario, un servicio automático llamado DNS convierte automáticamente esos crípticos números IP a palabras más inteligibles (como www.universidad.edu) para que sean fáciles de recordar.

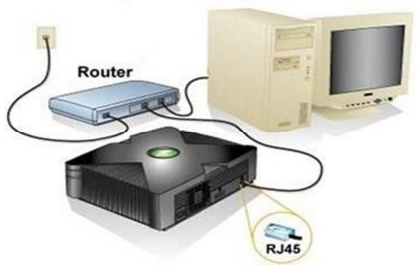
Toda Internet funciona a través de TCP/IP, y razones históricas hacen que está muy ligado al sistema operativo Unix (y sus variantes).

Por fortuna, los usuarios actuales no necesitan tener ningún conocimiento de los crípticos comandos Unix para poder navegar por la Red: todo lo que necesitan es un ratón.

1.5.4. Conexión

Generalmente se accede a Internet a través de la línea telefónica, pero también es posible hacerlo mediante un cable de fibra óptica. Si la línea telefónica dispone de un conector en la pared para instalar el teléfono, también se puede conectar a él un MODEM que salga de la computadora. Para seguir conectado y mientras hablar por teléfono, casi todos los módems tienen dos conectores: teléfono y línea. La conexión a Internet requiere disponer de cinco elementos: una computadora, un MODEM, un programa que efectúe la llamada telefónica, otro programa para navegar en la Red y una empresa proveedora de Internet que realice la función de servidor o intermediario.

Figura No. 17: Conexión

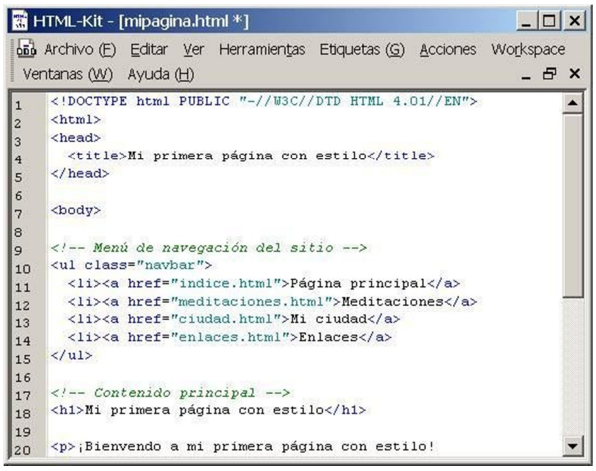


1.5.5. HTML Hiper Text Market Language

Estas siglas significan Hiper Text Markup Language (Lenguaje de Marcas de Hipertextos). Es el que permite saltar de una página a otra en un mismo documento o hacia otro que podría está localizado al extremo opuesto del planeta.

A estos textos, que no son continuos ni lineales y que se pueden leer como saltando las páginas hacia cualquier lado se les llama hipertexto o hipermedia (expresión que comprende todos los contenidos posibles, es decir, textos, audio, imágenes, iconos y vídeos). Los browser o navegadores permiten visualizar la forma amena y atractiva, toda la información en la pantalla del monitor.

Figura No. 18: HTML



1.5.6. Internet

Uno de los usos más obvios es el del correo electrónico: enviar y recibir mensajes a cualquier otra persona conectada sin necesidad de cartas, teléfonos, faxes o contestadores, con la ventaja de recibir información editable o archivos especiales (de tratamiento de texto, hojas de cálculo, etc.) con los que trabajar. El correo electrónico es rápido y efectivo, y al haberse convertido en algo global, es casi tan importante como el fax o el teléfono.

Figura No. 19: Internet

Otra de las utilidades más comunes es el entretenimiento: los usuarios encuentran en los grupos de noticias de Usenet, en las listas de correo y en el IRC una forma de comunicarse con otras personas con las que comparten intereses y aficiones. No tienen por qué ser necesariamente temas técnicos: hay grupos de charlas sobre cualquier tema imaginable, desde las más modernas técnicas de programación de ordenadores hasta series de televisión, y grupos de aficionados a un tipo determinado de coches o música. Están presentes los que examinan detalle a detalle series de televisión o películas, o los que adoran la ciencia o el arte. También hay mucha

información para grupos específicos de personas que pertenecen a grupos marginales y que de otro modo ven limitada su comunicación, así como infinidad de proyectos de participación.

Para los usuarios de ordenadores personales, Internet está repleta de archivos y programas de distribución pública, que pueden usar de forma gratuita (o del tipo "paga-si-te-gusta"), incluyendo utilidades, aplicaciones y juegos.

Internet también se presenta como un vasto almacén de información. Hay miles de bases de datos y recopilaciones de información sobre todos los temas imaginables: médicos, históricos, periodísticos y económicos.

Se puede acceder a la bolsa en tiempo real y a los periódicos del día. Los documentos FAQ (Preguntas frecuentes) recogen para los principiantes todas las preguntas habituales sobre asuntos concretos, desde el paracaidismo hasta la magia o la programación en C++, y son una fuente inagotable de información junto con los archivos de mensajes públicos de Usenet. Las empresas incluyen su información corporativa y de productos en la World Wide Web, hay bibliotecas con libros y artículos de revistas, y cada vez son más los periódicos y agencias de noticias que lanzan sus materiales a Internet.

En general, el ámbito universitario es el que más se beneficia de Internet: se puede investigar en profundidad cualquier tema imaginable, localizar artículos y personas de todo el globo que compartan proyectos e intereses, y establecer con ellos una comunicación diaria. Y aunque no sea usted estudiante, toda esa información está allí para que pueda buscarla y usarla.

Las empresas usan Internet para dar a conocer sus productos y servicios, para hacer publicidad y para estar más cerca de sus clientes o usuarios. Los particulares la usan también para publicar cualquier información que consideran interesante o creativa, y es sorprendente lo bien que funciona el hecho de que cualquier persona, con muy pocos medios, pueda convertirse en su propio editor de materiales multimedia.

1.5.7. Web

La World Wide Web (la "telaraña" o "maraña mundial") es tal vez el punto más visible de Internet y hoy en día el más usado junto con el correo electrónico, aunque también es de los más recientes. Originalmente denominado Proyecto WWW y desarrollado en el CERN suizo a principio de los 90, partió de la idea de definir un "sistema de hipermedios distribuidos."

Figura No. 20: Web

La WWW puede definirse básicamente como tres cosas: hipertexto, que es un sistema de enlaces que permite saltar de unos lugares a otros; multimedia, que hace referencia al tipo de contenidos que puede manejar (texto, gráficos, vídeo, sonido y otros) e Internet, las base sobre las que se transmite la información.

El aspecto exterior de la WWW son las conocidas "páginas Web." Una ventana muestra al usuario la información que desea, en forma de texto y gráficos, con los enlaces marcados en diferente color y subrayados. Haciendo un clic con el ratón se puede "saltar" a otra página, que tal vez esté instalada en un servidor al otro lado del mundo. El usuario también puede "navegar" haciendo pulsando sobre las imágenes o botones que formen parte del diseño de la página.

Las páginas de la WWW están situadas en servidores de todo el mundo (sitios Web), y se accede a ellas mediante un programa denominado "navegador"
(browser). Este programa emplea un protocolo llamado HTTP, que funciona sobre TCP/IP, y que se encarga de gestionar el aspecto de las páginas y los enlaces.

Cada página Web tiene una dirección única en Internet, en forma de URL. Un URL indica el tipo de documento (página Web o documento en formato HTML), y el de las páginas hipertexto de la WWW comienza siempre por http.

La Web proporciona algunas opciones interesantes: se puede circular saltando de un sitio a otro y volviendo rápidamente a los sitios que se acaban de visitar. La información puede presentarse en forma de tablas o formularios. El usuario puede en esos casos completar campos (por ejemplo, una encuesta) y enviarlos por correo electrónico con sólo hacer clic sobre el botón "enviar" que ve en su pantalla. La Web también facilita el acceso a información gráfica, películas o sonido de

forma automática.

La Web es el lugar de Internet que más crecimiento está experimentando últimamente: se calcula que hay más de 50 millones de páginas Web en la Red, y su número crece a un ritmo vertiginoso. La Web, al facilitar la búsqueda de información, ha hecho que otros servicios de Internet como Gopher, Archie o WAIS se usen cada vez menos.

Cada vez son más las empresas que publican información en la Web. Y encontrarla es también cada vez más fácil: casi todos los nombres de los sitios Web comienzan por el URL que indica que se trata una página Web en formato HTML (http://) seguido de las letras características de la Web (WWW), el nombre de la empresa (por ejemplo, .IBM) y terminan con el identificador de empresa (.com) o país (.es).

Es decir, si usted conecta con http://www.ibm.com visitará las páginas de IBM en Estados Unidos, y con http://www.ibm.es, las de IBM España. Pocas son las empresas de gran tamaño que no tienen su propia página Web hoy en día. Parte de la gran potencia de la Web también proviene del hecho de que cada vez es más fácil publicar material en la Web e Internet, no sólo acceder a lo que ya está allí. Existen programas gratuitos y comerciales para crear páginas HTML para la Web (similares a los programas de autoedición, sin necesidad de programación), y alquilar espacio en un servidor al que enviar las páginas es cada vez más barato y accesible. Hoy en día, cualquiera puede publicar cualquier lo que desee con un mínimo esfuerzo, y ponerlo al alcance de millones de personas.

1.5.8. Aspectos tecnológicos deInternet

Para tener una idea clara del concepto de WWW, es fundamental tener algunas nociones básicas sobre lo que es Internet. Internet es el nombre que recibe la red de ordenadores más extensa que existe en la actualidad. Se trata, en realidad, de una red de redes interconectadas que, gracias a unas normas y estándares comunes pueden comunicarse e intercambiar información todos los ordenadores conectados a dicha red. La arquitectura que da soporte a Internet es la denominada cliente/servidor, esto es, unos ordenadores almacenan la información (los ordenadores servidores) y otros acceden a ella (los ordenadores clientes).

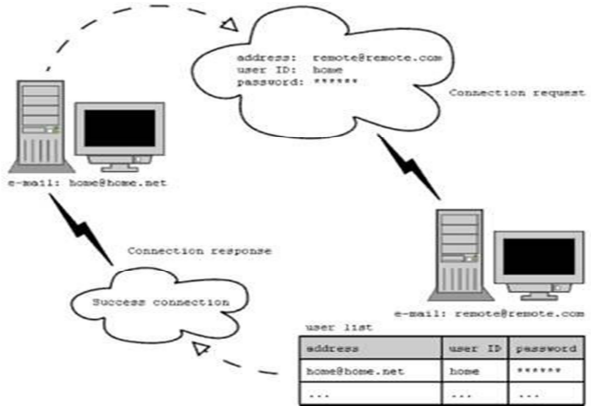
Figura No. 21: Ordenadores

El protocolo más básico de Internet -o paquete de protocolos- es el protocolo TCP/IP (Transfer Control Protocol/Internet Protocol). Cualquier otro protocolo de Internet se basa en IP o le sirve de base.

El funcionamiento del protocolo TCP/IP es el siguiente. Primero, el protocolo TCP (Transmision Control Protocol) fragmenta los datos en paquetes de información. Después, estos paquetes son enviados a la red, posiblemente sobre rutas diferentes, según el IP (el Protocolo de Internet). Finalmente, estos paquetes se vuelven a recomponer en el destino (o se restauran en caso de corrupción o pérdida de datos) en su orden correcto de llegada.

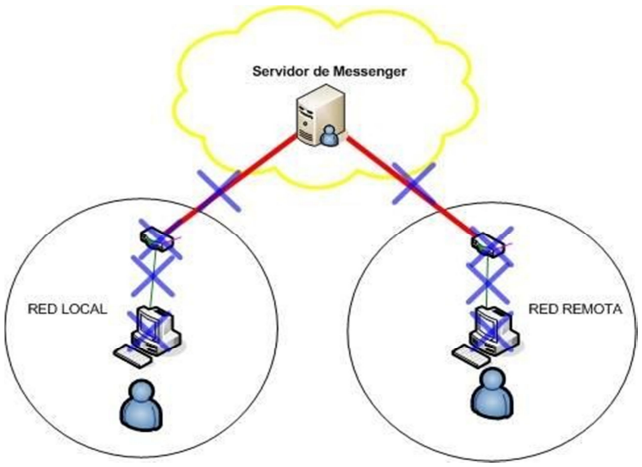
Para que sea posible la comunicación entre ordenadores, es necesario que cada máquina posea una identificación única. Así, cada ordenador conectado a Internet tiene un número IP y una DNS (Domain Name Server), el primero se expresa con números y el segundo con letras.

Figura No. 22: IP, DNS



En el contexto de Internet, el ordenador es más que un dispositivo para el cómputo o para el procesamiento de textos, se trata de un instrumento que suministra una plataforma para el sistema operativo y para las aplicaciones de software que soportan la transmisión de información en red y su utilización por parte del usuario

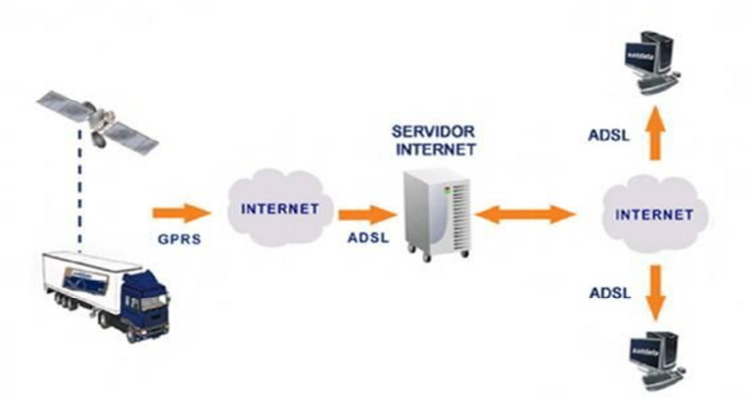
Figura No. 23: Servidores

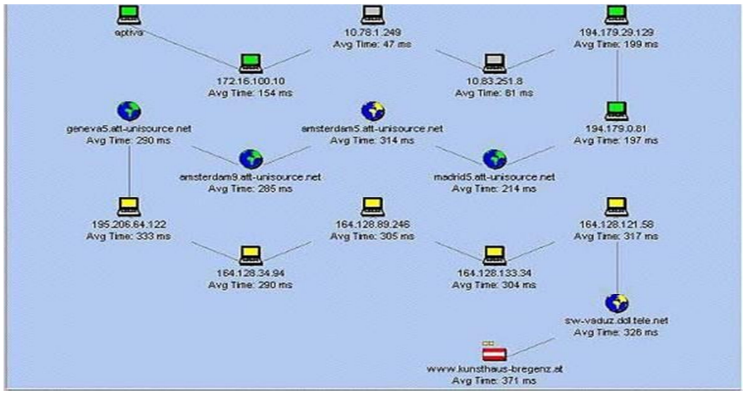


En Internet, las relaciones entre ordenadores siguen comúnmente el modelo de servidor-cliente. Igual que los protocolos TCP/IP, el modelo de servidor-cliente es una característica que homogeniza la comunicación en Internet. Un servidor es un ordenador junto con un hardware asociado y las aplicaciones de software que actúan como un depósito para los archivos de la información o los programas de software.

El servidor envía esta información respondiendo a una petición de los usuarios del software cliente a través de la red.

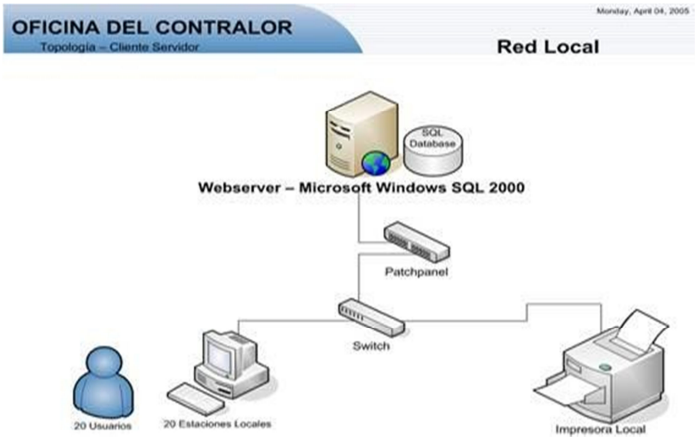
Figura No. 24: Servidor





La comunicación de servidor-cliente también sigue un conjunto de protocolos. Estos protocolos definen un uso particular que usan cliente y servidor. Por ejemplo, el protocolo Gopher de Internet, hoy en desuso, definía un uso para estructurar la información en un sistema de menús, submenús y entradas. Un usuario de un cliente Gopher hacía una petición para obtener una lista de artículos de menú a un servidor Gopher. El servidor Gopher devolvía esta lista y el cliente Gopher mostraba la lista al usuario. En la actualidad, esta misma función la realiza el protocolo HTTP de la World Wide Web.

Figura No. 25: Protocolos



Los distintos protocolos más utilizados son: la transferencia de archivos, el correo electrónico y el protocolo de la Web, pero existen otros muchos. Cada uno cuenta con aplicaciones clientes que hacen más fácil su uso.

La forma distribuida de servidor-cliente funciona muy eficazmente, ya que el software de cliente actúa recíprocamente con el servidor según un protocolo de intercambio de datos estándar. El servidor no tiene que "preocuparse" del hardware o las particularidades de software del ordenador sobre el que el que reside el software del cliente. Por su parte, el software del cliente no tiene que "preocuparse" de cómo solicita la información un tipo particular de servidor, puesto que todos

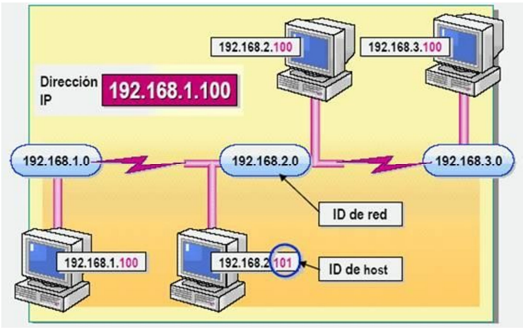
los servidores de un protocolo particular se comportan de la misma forma.

Por ejemplo, un cliente de Web que puede tener acceso a cualquier servidor de Web puede ser desarrollado para ordenadores Macintosh. Este mismo servidor de Web podría ser accedido por un cliente de Web soportado sobre un terminal de trabajo Windows que controla un sistema Unix. Esto hace más fácil desarrollar la información porque las versiones de la información distribuida de un servidor no tienen que ser desarrolladas para una plataforma de hardware particular. Todas las personalizaciones necesarias para el ordenador del usuario se escriben en el software del cliente para aquella plataforma.

El modelo de servidor-cliente es la característica clave para la comunicación en Internet. Un mensaje sobre Internet es codificado, almacenado y transmitido según las reglas de uso del servidor-cliente y el paquete de protocolos TCP/IP.

Para acceder a los archivos concretos dentro de un servidor es necesario conocer dónde están ubicados estos y para ello es preciso dotarlos de una dirección. Esta dirección es la URL o Universal Resource Locator) que está compuesta de los siguientes elementos: el protocolo seguido del signo de dos puntos y una doble barra inclinada, nombre de la máquina (número IP o DNS), directorio y subdirectorios, y archivo.

Figura No. 26: Números IP O DNS



http://www.hipertexto.info/internet_tegn.htm

Veamos con más detalle algunos de los conceptos básicos que hay que conocer para comprender Internet:

Figura No. 27: Protocolos

PROTOCOLOS	OTROS CONCEPTOS BÁSICOS
• TCP/IP • FTP • HTTP • SMTP (mail) • NNTP (news) • IRC • TELNET • GOPHER	URLs Direcciones IP DNS (Domain Name System) Nombres de dominio Principales organismos de Internet Organismos a nivel global

1.6. PROTOCOLOS

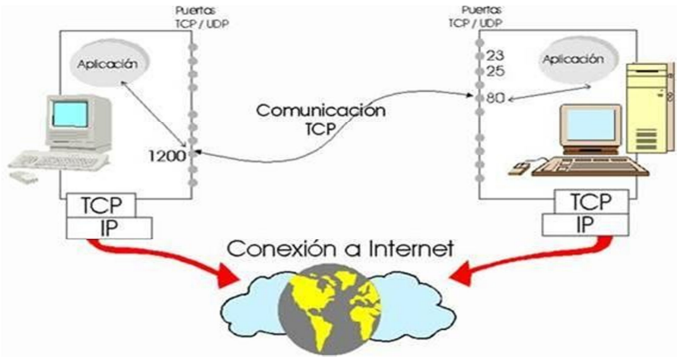
En informática, un protocolo no es más que un conjunto de reglas formales que permiten a dos dispositivos intercambiar datos de forma no ambigua. Un protocolo es, pues, un conjunto de reglas que permiten intercambiar información. El ordenador conectado a una red usa protocolos para permitir que los ordenadores conectados a la red puedan enviar y recibir mensajes, y el protocolo TCP/IP define las reglas para el intercambio de datos sobre Internet. Este conjunto de protocolos, al principio se desarrolló para un proyecto de investigación del Departamento de Defensa de los Estados Unidos, e integra un conjunto de servicios (que incluyen correo electrónico, la transferencia de archivos y la conexión remota) y que puede establecerse entre muchos ordenadores sobre una red local o en redes de un área más amplia.

Figura No. 28: Ordenadores

Las redes conectadas por donde pasa el paquete de protocolos TCP/IP son sumamente robustas. Si una sección de la red (o un servidor de ordenador en la red) se convierte en inoperativo, los datos pueden ser desviados sin causar daño a la red. La homogeneidad del protocolo es la esencia de la comunicación de Internet en el nivel de los datos. Mediante la cooperación de las conexiones de redes y el protocolo TCP/IP pueden conectarse sistemas de comunicación más y más grandes.

Las organizaciones individuales pueden controlar su propia red TCP/IP (internet) y conectarla con otras redes de Internet locales, regionales, nacionales y globales. Internet comparte el paquete de protocolos TCP/IP, sin embargo, Internet no es una red, sino una red de redes, un sistema organizado y distribuido cooperativamente a escala mundial para intercambiar información.

Figura No. 29: Conexión internet



Internet no es la única red global, hay otras redes globales que emplean protocolos diferentes, pero pueden intercambiar datos con Internet mediante puntos de intercambio llamados galerías o gateways. La comunicación de redes que no son Internet y que fluye en un punto de entrada es traducida a protocolos de comunicaciones de Internet y reexpedida a su camino, indistinguible de los paquetes que crea TCP enviando un mensaje directamente sobre Internet. De la misma manera, la comunicación puede fluir de Internet a otros puntos de entrada o gateways de la misma manera: los paquetes de Internet son traducidos a los protocolos de no-Internet necesarios para la comunicación sobre la otra red.

El correo electrónico es una forma popular de comunicación que se realiza a través de estas galerías o gateways. Mediante las gateways de correo electrónico, los usuarios sobre Internet pueden intercambiar correo electrónico con otros usuarios sobre redes que no son de Internet, como las que se utilizaban en los primeros tiempos de la red como BITNET (Because Its Time Network), UUCP (Unix-Unix Copy Protocol), y FidoNet (red basada en la comunicación de PCs sobre líneas telefónicas). Los usuarios de Internet también pueden intercambiar correo

electrónico con muchos servidores. El resultado es que el correo electrónico se disemina libremente en todas partes de Internet, así como en muchas otras redes. La colección resultante de redes mundiales que intercambian correo electrónico ha sido denominada Matrix.

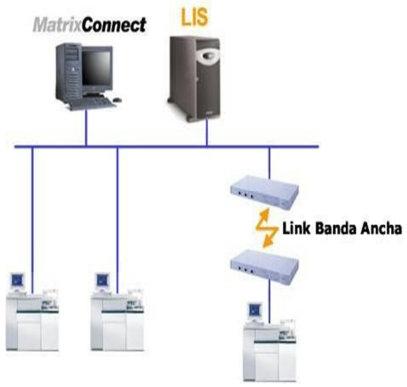
Aunque el flujo libre de correo electrónico haga difícil la distinción entre la comunicación de Internet y la comunicación de no-Internet en Matrix, la distinción entre Internet y Matrix para muchas otras formas de comunicación es crucial. Por ejemplo, la comunicación que usaba el protocolo Gopher de Internet no puede ser compartida fácilmente fuera de Internet. Asimismo Telnet, FTP (el Protocolo de Transferencia de Archivos) y la comunicación de World Wide Web está restringida, en la mayor parte de casos, a los usuarios de Internet. Los servicios comerciales en línea, reconociendo el valor de acceso a Internet para sus clientes, han estado creando más clases de entradas (gateways) a Internet que permiten a sus usuarios tener acceso a Telnet, FTP y la World Wide Web en Internet.

El resultado de esta mezcla de redes globales ha hecho que el protocolo de Internet se convierta en una especie de lengua franca del ciberespacio, creando puntos en común con otras muchas redes en línea que se unen mediante las susodichas gateways.

Los protocolos TCP/IP permanecieron bajo secreto militar hasta 1989. La World Wide Web llegó en 1991.

Los protocolos son, pues, una serie de reglas que utilizan los ordenadores para comunicarse entre sí. El protocolo utilizado determinará las acciones posibles entre dos ordenadores. Para hacer referencia a ellos en el acceso se escribe el protocolo en minúsculas seguido por "

Figura No. 30: Protocolo



http://www.hipertexto.info, **ftp://**ftp.hipertexto.info, etc.

1.7. TCP/IP. TANSMISION CONTROL PROTOCOL/INTERNET PROTOCOL:

Transmision Control Protocol o Protocolo de Control de Transmisión fragmenta los datos en paquetes de información. Después, estos paquetes son enviados a la red, posiblemente sobre rutas diferentes. El IP es el protocolo más básico de Internet, y provee todos los servicios necesarios para el transporte de datos. Cualquier otro protocolo de Internet se basa en IP o le sirve de base.

Fundamentalmente IP provee:

- **Direccionamiento:** Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los enrutadores (routers) para decidir el tramo de red por el que circularán.
- **Fragmentación:** Si la información a transmitir ("datagramas") supera el tamaño máximo "negociado" (MTU) en el tramo de red por el que va a circular podrá ser dividida en paquetes más pequeños, y reensamblada luego cuando sea necesario.
- **Tiempo de Vida de Paquetes:** Cada paquete IP contiene un valor de Tiempo de Vida (TTL) que va disminuyendo cada vez que un enrutador recibe y reenvía el paquete. Cuando este valor llega a ser de cero, el paquete deja de ser reenviado (se pierde).
- **Tipo de Servicio:** Este es un valor sin definición previa pero que puede indicar, por ejemplo, la prioridad del paquete.
- **Otras opciones:** Valores sin contenido definido previamente que se pueden utilizar, por ejemplo, para que la máquina de origen especifique la ruta que debe seguir el paquete, o para que cada enrutador agregue su propia dirección (para realizar seguimiento de ruta), o para indicar opciones de seguridad de la información contenida, etc.

El IPv6 será la próxima generación de protocolos de Internet y ya está en marcha. Este protocolo se ha desarrollado para ampliar la capacidad de conexión debido al crecimiento de dispositivos y al aumento de equipos portátiles. Y así, ofrecerá la infraestructura necesaria para teléfonos móviles, agendas PDA, electrodomésticos, etc.

La mayor diferencia entre la versión de IP utilizada actualmente (IP versión 4) e IPv6 radica en el espacio de direcciones más grande que admite IPv6. IPv6 admite direcciones de Internet de 128 bits, mientras que IP (versión 4) lo hace a 32 bits, además de ofrecer una configuración más simple y una mayor seguridad.

Por su parte, el protocolo TCP proporciona un servicio de comunicación que forma un circuito, es decir, hace fluir los datos entre el origen y el destino para que sea continuo. Este circuito virtual es lo que se denomina conexión. Así, TCP conecta los ordenadores o programas -loa llamados y los que llaman-, chequea los errores, controla el flujo y tiene capacidad para interrumpirlos.

FTP: File Transfer Protocol o Protocolo de transferencia de archivos . Es un protocolo que define cómo transferir archivos de un ordenador a otro, de un servidor remoto a un servidor local o viceversa. Se precisa un servidor de FTP y un cliente de FTP. Los servidores pueden ser de libre acceso con un login o FTP anónimo. El FTP anónimo es un servidor público de FTP al cual tiene acceso cualquier usuario de Internet sin necesidad de utilizar ninguna contraseña. Se puede utilizar desde un navegador web aunque hay programas específicos como CuteFTP. La mayoría de las páginas web son "subidas" a los servidores respectivos utilizando este protocolo para transferir los archivos desde el ordenador que ha confeccionado las páginas web hasta el servidor.

Figura No. 31: Bases de datos

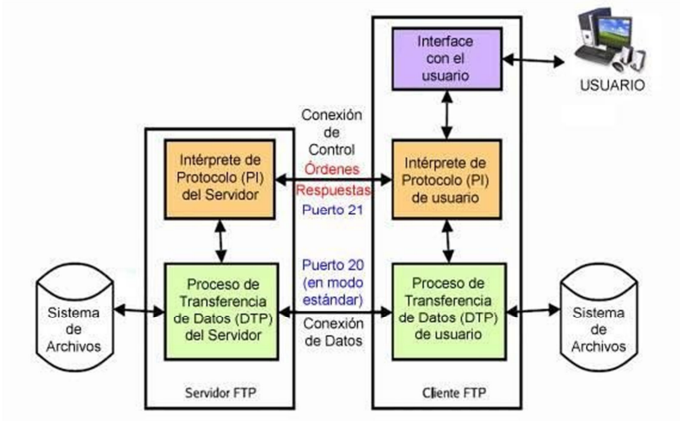


Diagrama del modelo FTP de transferencia de archivos

HTTP: HyperText Transfer Protocol o Protocolo de Transferencia de Hipertextos. Es el protocolo utilizado por los servidores de la World Wide Web desde el nacimiento de la Web en 1990. El protocolo HTTP es el que permite el intercambio de información hipertextual (enlaces) de las páginas web. Se trata de un protocolo genérico orientado a objetos, que puede usarse para muchas tareas como servidor de nombres y sistemas distribuidos orientados a objetos, por extensión de los comandos o los métodos usados. Una de sus características principales es la independencia en la visualización y presentación de los datos, lo que permite que los sistemas sean construidos independientemente del desarrollo de nuevos avances en la representación de los datos. Para visualizar los datos de la Web se precisa de un navegador instalado en la máquina del ordenador

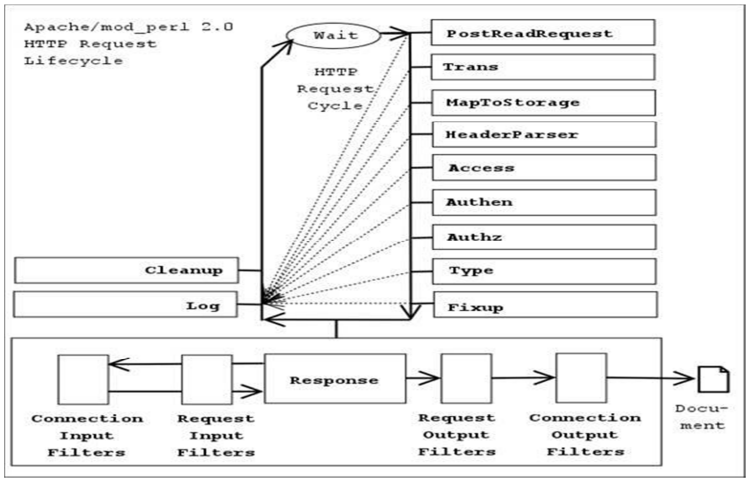
cliente. En este protocolo existen una serie de conceptos tales como:

- Conexión: es el circuito virtual establecido entre 2 programas en una red de comunicación
- Mensaje: es la unidad básica de un protocolo HTTP y consiste en una secuencia estructurada que se tramite entre los programas
- Cliente: es el programa que hace la llamada al servidor y es el que atiende en la transmisión la trama de los mensajes
- Servidor: es el programa que presta el servicio en la red
- Proxy: se trata de un programa intermedio que actúa sobre el servidor y el cliente
- Así, pues, el protocolo HTTP se basa en la conexión entre cliente y servidor.

Una transacción HTTP consiste básicamente en:

- Conexión: establecimiento de una conexión del cliente con el servidor. El puerto TCP/IP 80 es el puerto más conocido, pero se pueden especificar otros puertos no reservados.
- Solicitud: envío por parte del cliente de un mensaje de solicitud al servidor.
- Respuesta: envío por parte del servidor de una respuesta al cliente.
- Cierre: fin de la conexión por parte del cliente y el servidor.

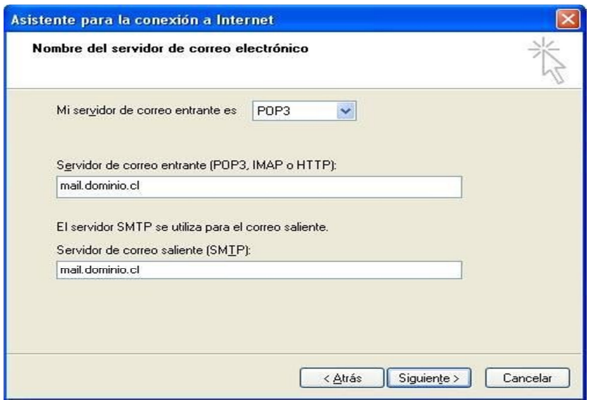
Figura No. 32: Transmisión HTTP



SMTP (mail) EL SMTP Simple Mail Transfer Procol o Protocolo de Transmisión de Correo Simple es el protocolo que nos permite recibir correos electrónicos y, junto con el protocolo POP (Post Office Protocol) o Protocolo de Oficina de Correos, usado por los ordenadores personales

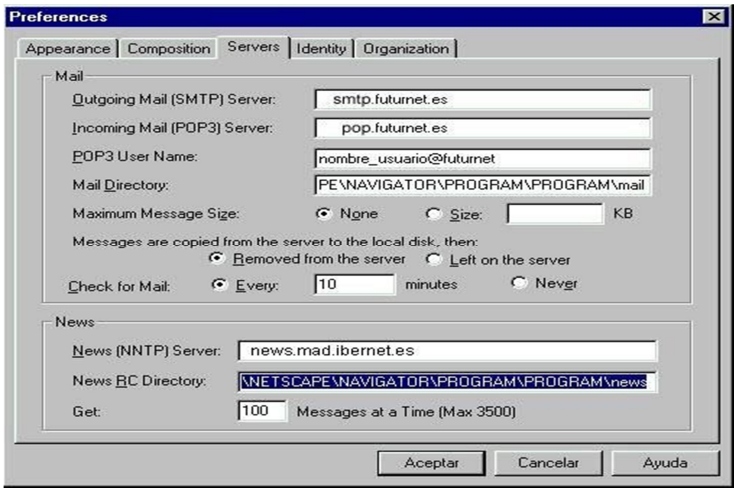
para administrar el correo electrónico, nos permitirá bajarnos los mensajes a nuestro ordenador. Para la mensajería instantánea se usa ahora el protocolo IMAP Internet Messagins Access Protocol (Protocolo de mensajería instantánea en Internet), más sofisticado que el protocolo POP.

Figura No. 33: Asistente conexión



NEWS (NNTP): Network News Tranfer Protocol. Protocolo de transferencia de sistemas de redes de news o noticias. Se trata de un foro de discusión por temas en forma de tablón de anuncios que cuenta con sus propios servidores y sus propios programas. Generalmente, el mismo programa que gestiona correos electrónicos, sirve para gestionar las news o noticias.

Figura No. 34: NNTP



IRC: IRC o Internet Relay Chat es un protocolo de comunicación que permite conversaciones (chats) y debates en grupo o en privado, en tiempo real siguiendo la arquitectura del modelo cliente-servidor, pero formándose redes entre los servidores para acoger a más usuarios. Las conversaciones se desarrollan en los denominados canales de chat. Se entra en ellos adoptando un nickname o apodo y existen personas encargadas de crear y mantener los canales (los llamados

CS o Chan Service), personas encargadas de mantener la red (IRCop), usuarios con privilegios de administrador del canal (Op) e incluso robots (Bot) que automatizan los servicios del canal. Existen muchos servidores de IRC. Algunos de ellos son: irc.

Para acceder a uno de estos servicios como usuario se requiere de un programa o cliente de IRC. Actualmente este servicio también se presta a través de la interfaz de la World Wide Web y existen también otros programas de mensajería integral que permiten conjuntamente prestaciones de mensajería rápida, correo electrónico, audio conferencia, videoconferencia, asistencia remota y otras prestaciones.

Figura No. 35: INTERFACES

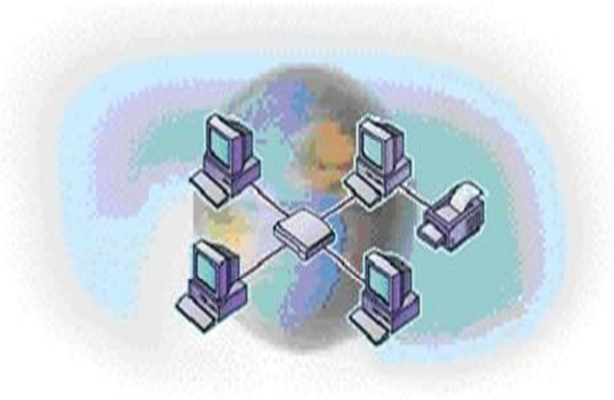
TELNET: Protocolo que permite la conexión remota a otro ordenador y que permite manejarlo como si se estuviese físicamente ante él. Así, es posible arreglar fallos a distancia o consultar datos en la otra máquina.

Ha sido un sistema muy utilizado por las grandes bibliotecas y centros de documentación como modo de acceso a sus catálogos en línea. Dejó de usarse hace unos años, cuando apareció y se popularizó el SSH (Secure Shell), que puede describirse como una versión cifrada de telnet. Uno de los mayores problemas de TELNET era la seguridad, ya que los nombres de usuario y contraseñas viajaban por la red sin cifrar. Para que la conexión funcionara, la máquina a la que se accede debía tener un programa especial que recibía y gestionaba las conexiones. El programa, al igual que el protocolo, también se denomina TELNET

Figura No. 36: Usuarios internet

GOPHER: Es un sistema de entrega de información distribuido, que en la actualidad se ha dejado de utilizar. Al utilizando era posible acceder a información local o bien a servidores de información gopher de todo el mundo. Permitía establecer una jerarquía de documentos, y búsquedas en ellos por palabras o frases clave. Su nombre se debe a la mascota -un topo- de la Universidad de Minessotta, donde fue creado, aunque otros autores sugieren que es una deformación de la frase goes-fer (busca). Fue el precursor de la Web al resolver el resolver el problema de cómo ubicar los recursos en Internet reduciendo todas las búsquedas a menús y submenús.

Figura No. 37: GOPHER



URL Otros conceptos básicos urls (unit resource locator)

La dirección completa de una página web se denomina URL (Uniform Resource Locator) o localizador uniforme de recursos, mientras que la dirección del servidor se conoce como DNS (Domain Name System) o nombre de dominio.

La URL no es más que la dirección electrónica para poder acceder a un recurso en un servidor remoto. Los siguientes esquemas son algunos reconocidos por la RFC (Request For Comments) y aprobados por la Internet Society (ISOC):

- ftp - "File Transfer protocol"
- http - "HyperText Transfer Protocol"
- gopher - El protocolo Gopher
- mailto - Dirección de Correo Electrónico
- news - "USENET news"
- nntp - "USENET news" usando acceso NNTP
- telnet - Sesiones interactivas
- wais - "Wide Area Information Servers"
- file - Nombres de fichero específicos de un host

Como para visualizar las páginas web se emplea el protocolo HTTP (Hypertext Transfer Protocol), normalmente los navegadores asumen por defecto el protocolo HTTP y no es necesario teclear http:// al introducir las direcciones URL, sin embargo, como ya hemos afirmado, también se emplean otros protocolos como el FTP,

Los nombres pueden ser muy largos o muy sencillos, dependiendo de la ruta de los directorios y subdirectorios que hay que seguir para localizar la página:

Protocolo/Nombre de dominio internacional/ Directorio/ Subdirectorio/ Subdirectorio/ Archivo
Hablamos de una URL absoluta cuando la dirección completa de Internet correspondiente a una página o recurso de la World Wide Web. La dirección URL absoluta incluye un protocolo, como "http", una ubicación en la red y una ruta de acceso y un nombre de archivo opcionales. Por ejemplo, http://www.hipertexto.info es una dirección URL absoluta.

DNS (Domain Name System) La DNS (Domain Name System) o sistema de nombres de dominio es el que permite localizar una dirección en Internet. En realidad, el sistema de nombres de dominio se creó para facilitar la navegación, pues no es más que el alias de las direcciones IP, que al constar de grupos de cuatro números son difíciles de recordar. Cada dirección IP tiene, pues, asignado un nombre de dominio. (Se trata de un ejemplo ficticio).

Dirección IP: 121.120.10.1

La DNS consiste en una serie de tablas de equivalencias entre dominios y direcciones IP. Estas tablas están distribuidas por servidores repartidos en Internet y que se actualizan de forma continua. Los ordenadores permanentemente conectados a Internet (los servidores) tienen direcciones fijas, pero los que se conectan de forma ocasional (clientes) reciben una dirección IP de forma ocasional cada vez que se conectan por parte de sus respectivos servidores. Las palabras que forman un nombre de dominio responden a una jerarquía organizada de derecha a izquierda: Dominio 3er nivel. Dominio de 2º nivel. Dominio de 1er nivel (DNS: www.hipertexto.info, s.f.)

Figura No. 38: Propiedades del protocolo

Nombres de dominio

Figura No. 39: Nombres de dominio

DOMINIOS DE PRIMER NIVEL:	DOMINIOS GEOGRÁFICOS:
✓ **com** para compañías y empresas comerciales ✓ **net** para organizaciones relacionadas con Internet ✓ **org** para organizaciones que no se pueden clasificar en ninguna otra categoría ✓ **edu** para instituciones educativas (sólo lo suelen utilizar las universidades de EE.UU.) ✓ **gob** para el gobierno de EE.UU. ✓ **mil** para las Fuerzas Armadas de EE.UU. ✓ **biz** para negocios y empresas comerciales ✓ **info** para proveedores de servicios de información ✓ **name** para páginas personales	➢ **Es**, España ➢ **Fr**, Francia ➢ **Uk**, Reino Unido ➢ **Ca**, Canadá ➢ **It**, Italia ➢ **eu** Unión Europea (Existen unos 260 dominios de tipo geográfico).

CAPITULO II

2. EL PROCESO DE LA AUDITORÍA INFORMÁTICA

2.1. CONCEPTOS Y DESARROLLO

2.1.1. SGO DE AUDITORÍA

CONCEPTO.- Es el riesgo de que los estados financieros, área o actividad que se está examinando, contenga errores o irregularidades no detectadas una vez que la auditoría ha sido completada.

Los estados financieros pueden incluir: errores, fraude y actos ilegales.

- **Errores:** Fallas u omisiones no intencionales.
- **Fraude:** Actos intencionales que causan una falsificación en los estados financieros.
- **Actos ilegales:** Una auditoría efectuada conforme las NAGAS debería ofrecer una seguridad razonable de detectar efectos materiales directos.

Tipos De Riesgo:

Riesgo Inherente (RI).- Es la posibilidad de errores o irregularidades en la información financiera, administrativa u operativa, antes de considerar la efectividad de los controles internos diseñados y aplicados por el ente.

Riesgo de Control (RC).- Está asociado con la posibilidad de que los procedimientos de control interno, incluyendo a la unidad de auditoría interna, no puedan prevenir o detectar los errores e irregularidades significativas de manera oportuna.

Riesgo de Detección (RD).- Existe al aplicar los programas de auditoría, cuyos procedimientos no son suficientes para descubrir errores o irregularidades significativas.

Al planificar una auditoría, el auditor, basado en la evaluación del riesgo inherente y de control, deberá considerar suficientes procedimientos sustantivos para reducir el riesgo de detección.

2.1.2. CONTROL

Se entiende por control a todas las políticas, procedimientos, prácticas y estructura organizacional implementados con la finalidad de reducir Riesgos.

Son establecidas para proveer seguridad razonable de que los objetivos específicos serán alcanzados. Por tanto los controles apuntan a dos objetivos:

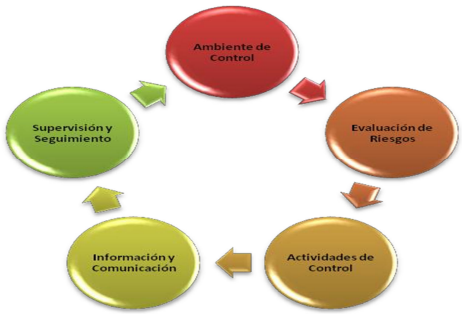
- Lo que debe ser alcanzado
- Lo que debe ser evitado

El control interno nace de la necesidad de evaluar u satisfacer la eficiencia, eficacia, razonabilidad, oportunidad y confiabilidad, en protección y seguridad de los bienes de la empresa, así como para ayudar a controlar el desarrollo de sus actividades operaciones u resultados financieros, que se espera obtener en el desempeño de las funciones u operaciones de toda la empresa.

Tipos De Control:

Control Interno.- Es un proceso aplicado por la máxima autoridad, la dirección y el personal de cada institución, que proporciona seguridad razonable de que se protegen los recursos y se alcancen los objetivos institucionales.

Elementos:



Tiempos de Control Interno.- El ejercicio del control interno se aplicará en forma previa, continua y posterior:

OBJETIVOS DEL CONTROL

Los objetivos que persigue el control, depende del tipo de entidad, donde se establezcan y a las

características específicas de las mismas, entre los mismos pueden estar:

a. Se adopta para establecer estándares, medir su cumplimiento y evaluar el alcance real de los planes y programas.
b. Protección y salvaguarda de los bienes y activos de la empresa.
c. Planear y evaluar el cumplimiento de las funciones, actividades y operaciones de la empresa.
d. Contribuir en la buena marcha de la empresa

ELEMENTOS DEL CONTROL

Los elementos del control interno son:

1. Elementos de organización: Dirección, coordinación, asignación de responsabilidades.
2. Elementos de procedimientos: Planeación y sistematización, registros y formas, informes.
3. Elementos de personal: Entrenamiento, eficacia eficiencia, moralidad y retribución.
4. Elementos de supervisión: Revisión para precisar, perdidas y deficiencias, mejores métodos, mejores formas de control, operaciones más eficientes, mejor uso de los recursos físicos y humanos.

ELEMENTOS DEL CONTROL INTERNO INFORMATICO

Los elementos fundamentales del control interno informático son:

1. Controles internos sobre las organizaciones en el área informática Dirección: coordinación de recursos, supervisión de actividades, delegación de autoridad y responsabilidad, asignación de actividades, distribución de recursos.

División del trabajo: Dirección general del área, área de análisis y diseño, área de programación, área de sistema de redes, área de operación, área de comunicaciones, área de administración.
Asignación de responsabilidad y autoridad: Son considerad a partir de la asignación de funciones.
Establecimiento de estándares y métodos: De las actividades y funciones, para que sean desarrolladas de manera uniforme, conforme a las necesidades propias de cada institución.
Perfiles de puesto: La forma de operación establecida para cada puesto, de acuerdo con los sistemas de cómputo de la empresa.

2. Controles sobre el análisis, desarrollo e implementación de sistemas: Análisis del sistema actual, diseño conceptual, diseño detallado, programación, pruebas y correcciones, documentación del sistema, capacitación de usuarios, implementación del sistema, liberación del sistema, mantenimiento.
3. Controles internos sobre las operaciones del sistema: establecer la prioridad de la seguridad y protección de la información, del sistema de cómputo y de los recursos informáticos de la empresa; promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en las empresas.
4. Controles internos sobre los procedimientos de entrada de datos, el procesamiento de la información y la emisión de resultados: Verificar la existencia y funcionamiento de los procedimientos de captura de datos, comprobar que los mismo sean debidamente procesados, así como determinar la confiabilidad, veracidad y exactitud del procesamiento de datos y comprobar la suficiencia en la emisión de información.
5. Controles internos sobre la seguridad física y de información del área de sistemas: seguridad física, seguridad lógica, seguridad de base de datos, seguridad en la operación, seguridad del personal de informática, seguridad de telecomunicaciones, seguridad en las redes, prevención de contingencias y riesgos.

2.1.3. AUDITORÍA

Es una herramienta de control y supervisión que contribuye a la creación de una cultura de la disciplina de la organización y permite descubrir fallas en las estructuras o vulnerabilidades existentes en la organización.

La Auditoría de Sistemas, es un examen de sistemas, programación y procesamiento del centro de datos con el objeto de determinar la eficiencia de las operaciones de computación.

2.2. METODOLOGIA DE AUDITORIA INFORMATICA

La metodología de las auditorias de sistemas, tiene tres etapas o fases, que se detalla a continuación:

1. Planeación de la auditoria de sistemas

    a. Identificar el origen de la auditoria
    b. Realizar la visita preliminar al área que será evaluada

c. Establecer los objetivos de la auditoria
d. Determinar puntos a evaluar
e. Elaborar planes, programas y presupuestos para realizar la auditoria
f. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoria
g. Asignar los recursos y sistemas computacionales para la auditoria

2. Ejecución de la auditoria

   a. Realizar las acciones programadas para la auditoria
   b. Aplicar instrumentos y herramientas planificadas
   c. Identificar y elaborar las desviaciones encontradas
   d. Elaborar el dictamen preliminar y presentarlo
   e. Integrar los papeles de trabajo

3. Dictamen de la auditoria

   a. Análisis de la información y elaboración del informe final
   b. Dictamen final
   c. Presentación del informe

2.3. PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA

2.3.1. Identificar el origen de la auditoria

Lo primero que se de identificar, el motivo por el cual nace la necesidad de una auditoría, por ello es este punto es necesario realizar las pregunta: qué? Cómo?, para qué? Se requiere evaluar algún aspecto de la empresa. Es muy importante identificar el origen, porque con ello se sabe que existirá el comprometimiento para la entrega de la información.

Dentro de este punto puede estar, la solicitud expresa interna o externa, emergencia o condiciones especiales, riesgos y contingencias informáticas, evaluación del plan de contingencia, acciones de mejora de auditoría anteriores o como parte del programa integral de auditoría.

Con la identificación se puede saber de antemano cuáles serán los aspectos primordiales en las evaluación es decir cuáles serán los asuntos más relevantes sobre los cuales se deberá trabajar.

2.3.2. Realizar la visita preliminar al área que será evaluada

Es recomendable que el auditor visite de manera preliminar el ´rea de informática que será auditada, después de conocer la petición de auditoría, y antes de empezar formalmente el examen.

Para ello el auditor debe, realizar una visita preliminar de arranque, en la que debe conocer t tomar el contacto inicial con los funcionarios y empleados del área, y con ello identificar la problemática de sistema, establecer objetivos y calcular los recursos y personas necesarias que integrarán el equipo auditor.}

2.3.3. Establecer los objetivos de la auditoria

Los objetivos deben representar condiciones futuras deseadas que incluyan propósitos, metas fines y plazos, a ser cumplidas por las personas y organizaciones.

El objetivo general debe enfocarse en todos los aspectos que se pretenden Evaluar, es decir se constituye en el fundamento de la realización de la auditoría.

Los objetivos particulares son fines individuales que se pretenden alcanzar en el desarrollo de la auditoria, y se refieren a un área específica.

2.3.4. Determinar puntos a evaluar

Es siguiente paso es determinar los puntos concretos a evaluar, y para ello se debe considerar, la gestión administrativa e informática del centro de datos, el cumplimiento de las funciones del personas informativo y usuarios de los sistemas, el análisis diseño y desarrollo de los sistemas, la operación, capacitación y adiestramiento del personal, la protección y niveles de acceso a las bases de datos, protección y respaldo de archivos, seguridad y protección de los usuarios.

2.3.5. Elaborar planes, programas y presupuestos para realizar la auditoria

Elaborar un documento formas de los planes de trabajo, que incluya los eventos que servirán de guía, la estimación de los recursos humanos, materiales e informáticos que serán utilizados, los tiempos estimados para para las actividades, los auditores responsables y participantes en dichas actividades y demás especificaciones del programa de trabajo.

2.3.6. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoria

Se refiere a definir las áreas y puntos de sistemas a ser evaluados y realizar las ponderaciones de auditoria: diseñar herramientas e instrumentos de recolección de datos, como cuestionarios, entrevistas, encuestas: elaborar formatos de levantamiento de información de inventarios, diseñar las pruebas de evaluación.

2.3.7. Asignar los recursos y sistemas computacionales para la auditoria

Los recursos de cualquier índole son limitados, por tal razón, que una vez que se analizó los puntos a evaluar, se deben identificar los recursos que se necesitarán para realizar la evaluación, siempre en concordancia con lo planeado.

Para ello se debe identificar el personal que integrará el equipo de auditore3s, el personal del área que será evaluado, el apoyo de los sistemas y equipos técnicos e informáticos, apoyos materiales y administrativos, apoyos materiales y administrativos, tales como mobiliario, equipos, materiales y útiles de oficina.

Determinados los recursos materiales, se debe determinar los recursos económicos sobre todo en lo que se refiere a movilización, viáticos, pasajes y otros gastos menores de cada integrante del equipo auditor.

2.3.8. Elaborar planes, programas y presupuesto

A continuación se debe realizar la planeación formal de la la uditoría de sistemas, en la que se concretarán los planes, programas yi el presupuesto para la correcto desarrollo de la auditoría, este procedimiento se verá materializado, en papel, en el que se delimitará las etapas, eventos, actividades y los tiempos de ejecución de cada una.

2.3.9. Identificar y seleccionar métodos, herramientas e instrumentos

Se debe identificar los documentos y medios que se deberán utilizar para la revisión, los mismo que estarán de acuerdo con la planificación realizada; para ello se debe establecer una guía de ponderación de los puntos a ser evaluados, definir las áreas y puntos de sistemas que serán evaluados, elaborar los documentos necesarios para la recopilación de información, así como desarrollar cuestionarios y guías de entrevistas, y modelos de inventarios.

2.4. EJECUCION DE LA AUDITORIA

Una vez realizada la planeación, la siguiente etapa es la ejecución, la misma que se desarrollará en función a las características y requerimientos concretos de la primera etapa.
A continuación se describen las actividades concretas de esta etapa:

2.4.1. Realizar las acciones programadas para la auditoria

Cada integrante del equipo auditor debe realizar las actividades asignadas, y en los plazos establecidos y a la utilización de recursos solicitados.

2.4.2. Aplicar instrumentos y herramientas planificadas

Conforme a la guía, se deben utilizar los instrumentos y herramientas elegidas, ya sean esta recopilación, observación, entrevistas, encuestas, entre otras.

2.4.3. Identificar y elaborar las desviaciones encontradas

Realizadas las actividades planificadas e identificadas los instrumentos de recopilación, se deben buscar las posibles desviaciones, y se procede a elaborar los documentos, en los cuales se anotan las situaciones encontradas y las causas que las originaron y sus posibles soluciones.

2.4.4. Elaborar el dictamen preliminar y presentarlo

Una vez que el auditor determinó la desviación de la evaluación, debe elaborar un documento que contenga a todas las desviaciones; una vez terminadas se debe comunicar a las personas involucradas, a fin de encontrar de manera conjunta la mejor solución

2.4.5. Integrar los papeles de trabajo

El auditor debe conservar los documentos en un solo lugar llamado legajo de papeles, en los que se ha aplicado cada uno de los instrumentos y técnicas planificas.

2.5. DICTAMEN DE LA AUDITORIA

El último paso de la auditoría, es la emisión del dictamen, en la cual se refleja el resultado final de la auditoría, para ello se debe realizara los siguiente:

2.5.1. Análisis de la información y elaboración del informe final

La actividad paralela a las deviaciones, es el análisis de los papeles de trabajo y el borrador de las situaciones detectadas, y notificadas, a partir de lo cual se debe elaborar las modificaciones pertinentes.

2.5.2. Dictamen final

El auditor debe elaborar el informe de auditoría y complementarlo con su opinión final, es decir su opinión, antes de presentarlo a los directivos del área de sistemas, para que conozcan la situación actual del área.

2.5.3. Presentación del informe

El último paso, es la presentación formal del dictamen de la auditoría, al más alto directivo de la empresa, con el propósito de evaluar los resultados, el informe de auditoría debe contener, la carta de presentación, el dictamen de auditoría, el informe de situaciones relevantes y los anexos y cuadros adicionales.

CAPÍTULO III

3. ESTRUCTURA CONCEPTUAL DEL CONTROL INTERNO SEGÚN COSO

3.1. COSO (COMMITTEOFSPONSORINGORGANIZATIONS)

El denominado "INFORME COSO" sobre control interno, publicado en EE.UU. en 1992, surgió como una respuesta a las inquietudes que planteaban la diversidad de conceptos, definiciones e interpretaciones existentes en torno a la temática referida.

Plasma los resultados de la tarea realizada durante más de cinco años por el grupo de trabajo que la TREADWAY COMMISSION, NATIONAL COMMISSION ON FRAUDULENT FINANCIAL REPORTING creó en Estados Unidos en 1985 bajo la sigla COSO (COMMITTEE OF SPONSORING ORGANIZATIONS).

El Comité de Organizaciones Patrocinadoras está integrado por las siguientes organizaciones:

- AICPA (Instituto Interamericano de Contadores Públicos Certificados)
- AAA (Asociación de Contadores Públicos Certificados)
- IIA (Instituto de Auditores Internos)
- FEI (Instituto de Ejecutivos de Finanzas)
- IMA (Instituto de Contadores Gerenciales)

3.2. EL INFORME COSO

El Informe COSO es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de control.

Debido a la gran aceptación de la que ha gozado, desde su publicación en 1992, el Informe COSO se ha convertido en el estándar de referencia.

Existen en la actualidad 2 versiones del Informe COSO. La versión del 1992 y la versión del 2004, que incorpora las exigencias de ley SarbanesOxley a su modelo.

Es un medio para un fin, no un fin en sí mismo. Efectuado por la junta directiva, gerencia u otro personal.

No es sólo normas, procedimientos y formas involucra gente aplicado en la definición de la estrategia y aplicado a través de la organización en cada nivel y unidad diseñado para identificar los eventos que potencialmente puedan afectar a la entidad y para administrar los riesgos, proveer seguridad razonable para la administración y para la junta directiva de la organización orientada al logro de los objetivos del negocio.

3.3. CONTROL INTERNO

3.3.1. Roducción

El Control Interno ha sido preocupación de las entidades, en mayor o menor grado, con diferentes enfoques y terminologías, lo que ha permitido que al pasar del tiempo se hayan planteado diferentes concepciones acerca del mismo, sus principios y elementos que se deben conocer e instrumentar en la entidad cubana actual que se encuentra en proceso de aplicación de la Resolución No. 297 – 2003 del Ministerio de Finanzas y Precios.

Hace tiempo los altos ejecutivos buscan maneras de controlar mejor las empresas que dirigen. Los controles internos se implantan con el fin de detectar, en el plazo deseado, cualquier desviación respecto a los objetivos de rentabilidad establecidos por la empresa y de limitar las sorpresas. Dichos controles permiten a la dirección hacer frente a la rápida evolución del entorno económico y competitivo, así como a las exigencias y prioridades cambiantes de los clientes y adaptar su estructura para asegurar el crecimiento futuro.

El sistema de control interno está entrelazado con las actividades operativas de la entidad y existe por razones empresariales fundamentales. Es más efectivo cuando los controles se incorporan a la infraestructura de la sociedad y forman parte de la esencia de la empresa. Mediante los controles "incorporados" se fomenta la calidad y las iniciativas de delegación de poderes. Se evitan gastos innecesarios y se permite una respuesta rápida ante las circunstancias cambiantes.
Los controles internos fomentan la eficiencia, reducen el riesgo de pérdida de valor de los activos y ayudan a garantizar la fiabilidad de los estados financieros y el cumplimiento de las leyes y normas vigentes.

El control interno se define como un proceso, efectuado por el personal de una entidad, diseñado para conseguir unos objetivos específicos. La definición es amplia y cubre todos los aspectos de control de un negocio, pero al mismo tiempo permite centrarse en objetivos específicos.

3.3.2. Definición

El Control Interno es un proceso integrado a los procesos, y no un conjunto de pesados mecanismos burocráticos añadidos a los mismos, efectuado por el consejo de la administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar una garantía razonable para el logro de objetivos incluidos en las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y políticas.
- Completan la definición algunos conceptos fundamentales:

Completan la definición algunos conceptos fundamentales

- El control interno es un proceso, es decir un medio para alcanzar un fin y no un fin en sí mismo.
- Lo llevan a cabo las personas que actúan en todos los niveles, no se trata solamente de manuales de organización y procedimientos.
- Sólo puede aportar un grado de seguridad razonable, no la seguridad total, a la conducción.
- Está pensado para facilitar la consecución de objetivos en una o más de las categorías señaladas las que, al mismo tiempo, suelen tener puntos en común.

Al hablarse del control interno como un proceso, se hace referencia a una cadena de acciones extendida a todas las actividades, inherentes a la gestión e integrados a los demás procesos básicos de la misma: planificación, ejecución y supervisión. Tales acciones se hallan incorporadas (no añadidas) a la infraestructura de la entidad, para influir en el cumplimiento de sus objetivos y apoyar sus iniciativas de calidad.

Según la Comisión de Normas de Control Interno de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), el control interno puede ser definido como el plan de organización, y el conjunto de planes, métodos, procedimientos y otras medidas de una institución, tendientes a ofrecer una garantía razonable de que se cumplan los siguientes objetivos principales:

- Promover operaciones metódicas, económicas, eficientes y eficaces, así como

productos y servicios de la calidad esperada.

- Preservar al patrimonio de pérdidas por despilfarro, abuso, mala gestión, errores, fraudes o irregularidades.
- Respetar las leyes y reglamentaciones, como también las directivas y estimular al mismo tiempo la adhesión de los integrantes de la organización a las políticas y objetivos de la misma.
- Obtener datos financieros y de gestión completos y confiables y presentados a través de informes oportunos.
- Para la alta dirección es primordial lograr los mejores resultados con economía de esfuerzos y recursos, es decir al menor costo posible. Para ello debe controlarse que sus decisiones se cumplan adecuadamente, en el sentido que las acciones ejecutadas se correspondan con aquéllas, dentro entro de un esquema básico que permita la iniciativa y contemple las circunstancias vigentes en cada momento.
- Por consiguiente, siguiendo los lineamientos de INTOSAI, incumbe a la autoridad superior la responsabilidad en cuanto al establecimiento de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica.
- Ambas definiciones (COSO e INTOSAI) se complementan y conforman una versión amplia del control interno: la primera enfatizando respecto a su carácter de proceso constituido por una cadena de acciones integradas a la gestión, y la segunda atendiendo fundamentalmente a sus objetivos.

3.3.3. IMPLEMENTACIÓN

La implementación del control interno implica que cada uno de sus componentes estén aplicados a cada categoría esencial de la empresa convirtiéndose en un proceso integrado y dinámico permanentemente, como paso previo cada entidad debe establecer los objetivos, políticas y estrategias relacionadas entre sí con el fin de garantizar el desarrollo organizacional y el cumplimiento de las metas corporativas; aunque el sistema de control interno debe ser intrínseco a la administración de la entidad y busca que esta sea más flexible y competitiva en el mercado se producen ciertas limitaciones inherentes que impiden que el sistema como tal sea 100% confiable y donde cabe un pequeño porcentaje de incertidumbre, por esta razón se hace necesario un estudio adecuado de los riesgos internos y externos con el fin de que el control provea una seguridad razonable para la categoría a la cual fue diseñado, estos riesgos pueden ser atribuidos a fallas humanas como la toma de decisiones erróneas, simples equivocaciones o confabulaciones de varias personas, es por ello que es muy importante la contratación de personal con gran capacidad profesional, integridad y valores éticos así como la correcta

asignación de responsabilidades bien delimitadas donde se interrelacionan unas con otras con el fin de que no se rompa la cadena de control fortaleciendo el ambiente de aplicación del mismo, cada persona es un eslabón que garantiza hasta cierto punto la eficiencia y efectividad de la cadena, cabe destacar que la responsabilidad principal en la aplicación del control interno en la organización debe estar siempre en cabeza de la administración o alta gerencia con el fin de que exista un compromiso real a todos los niveles de la empresa, siendo función del departamento de auditoria interna o quien haga sus veces, la adecuada evaluación o supervisión independiente del sistema con el fin de garantizar la actualización, eficiencia y existencia a través del tiempo, estas evaluaciones pueden ser continuas o puntuales sin tener una frecuencia predeterminada o fija, así mismo es conveniente mantener una correcta documentación con el fin de analizar los alcances de la evaluación, niveles de autorización, indicadores de desempeño e impactos de las deficiencias encontradas, estos análisis deben detectar en un momento oportuno como los cambios internos o externos del contexto empresarial pueden afectar el desarrollo o aplicación de las políticas en función de la consecución de los objetivos para su correcta evaluación.

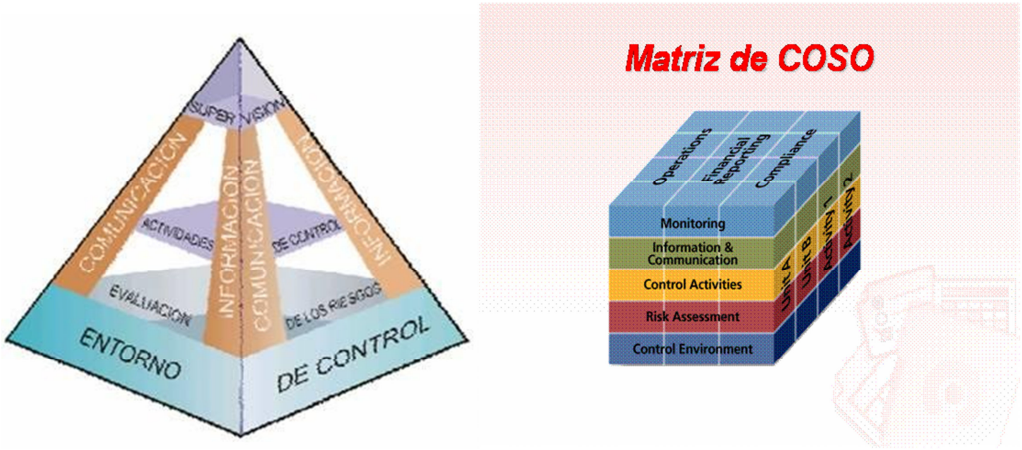
La comprensión del control interno puede así ayudar a cualquier entidad pública o privada a obtener logros significativos en su desempeño con eficiencia, eficacia y economía, indicadores indispensables para el análisis, toma de decisiones y cumplimiento de metas.

3.3.4. Commponentes del Control Interno

El marco integrado de control que plantea el informe COSO consta de cinco componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Supervisión

Figura No. 40: COSO



3.3.4.1. Importancia de los Componentes

¿Los cinco componentes del control interno son importantes?

Bueno, sino fueran importantes no existirían y el equipo multidisciplinario que elaboró el informe COSO no los hubiera analizado y expuesto tan exquisitamente, en dicho informe como los componentes del control interno.

Tampoco aparecieran en la Resolución No. 297-2003 del MFP como aspectos a desarrollar dentro del Sistema de Control Interno (SCI).

Vamos a hacer un análisis de la importancia de los cinco componentes mirándolos desde el punto de vista de los objetivos organizacionales y la interrelación que existe entre ambos. La definición, establecimiento y aplicación de los objetivos organizacionales es el requisito primario para poder introducir en la organización un SCI.

Los objetivos organizacionales te indican la dirección, te ubican, te dicen a donde ir. Deben ser enunciados por escrito definiendo los resultados a alcanzar en un periodo determinado. Los objetivos son el QUÉ: ¿Qué resultados queremos o necesitamos lograr?

3.3.4.2. Importancia de los Objetivos

Figura No. 41: Componentes y Objetivos

- ✓ Los objetivos proporcionan un sentido de dirección, sin ellos los individuos al igual que las organizaciones tienden a la confusión, reaccionan ante los cambios del entorno sin un sentido claro de lo que en realidad quieren alcanzar.
- ✓ Nos dicen cómo debe funcionar nuestro sistema, nos da la estructura, la organización.
- ✓ Nos ayudan a evaluar nuestro progreso pues un objetivo claramente establecido, medible y con una fecha específica, fácilmente se convierte en un estándar de desempeño que permite a los individuos evaluar sus progresos. Por lo tanto, los objetivos son una parte esencial del control.

De lo anterior se desprende que en una empresa debe dirigirse por objetivo, lo que significa que tanto los gerentes como los subordinados de una organización conjuntamente, identifican sus metas comunes, definen las áreas principales de responsabilidad de cada persona en término de los resultados que de él se esperan y emplear estas medidas como guías para el manejo de la unidad y para evaluar la contribución de cada uno de sus miembros.

Si los objetivos organizacionales te indican la dirección, hacia dónde ir, el resultado a lograr, los cinco componentes del control interno constituyen caminos para el logro de los objetivos de la organización, de los resultados planificados y el buen funcionamiento de la misma, coincidiendo con los objetivos esenciales de todo proceso de cambio que están enfocados al funcionamiento y los resultados empresariales.

Los componentes del control interno son el cuerpo del sistema y existen por las funciones que desarrollan cada uno de ellos. Proporcionan un grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías":

- ✓ Eficacia y eficiencia de las operaciones
- ✓ Fiabilidad de la información financiera
- ✓ Cumplimiento de las leyes y normas aplicables

3.3.4.3. Funciones Fundamentales de los Componentes

Para analizar cada componente partiremos del concepto dado en el Informe COSO sobre control interno: "el control interno se define como un proceso, efectuado por el personal de una entidad, diseñado para conseguir unos objetivos específicos. La definición es amplia y cubre todos los aspectos de control de un negocio, pero al mismo tiempo permite centrarse en objetivos específicos. El control interno consta de cinco componentes relacionados entre sí que son inherentes al estilo de gestión de la empresa. Estos componentes interrelacionados sirven como criterios para determinar si el sistema es eficaz", ayudando así a que la empresa dirija de mejor forma sus objetivos y ayuden a integrar a todo el personal en el proceso.

Ilustraremos de forma gráfica los cinco elementos que deben actuar en forma conjunta para que se pueda generar un efectivo control interno en las empresas.

Aunque los cinco criterios deben cumplirse, esto no significa que cada componente haya de funcionar de forma idéntica, ni siquiera al mismo nivel, en distintas entidades. Puede existir una

cierta compensación entre los distintos componentes, debido a que los controles pueden tener múltiples propósitos, los controles de un componente pueden cumplir el objetivo de controles que normalmente están presentes en otros componentes. Por otra parte, es posible que existan diferencias en cuanto al grado en que los distintos controles abarquen un riesgo específico, de modo que los controles complementarios, cada uno con un efecto limitado, pueden ser satisfactorios en su conjunto.

Existe una interrelación directa entre las tres categorías de objetivos, que son los que una entidad se esfuerza para conseguir, y los componentes, que representan lo que se necesitan para lograr dichos objetivos. Todos los componentes son relevantes para cada categoría de objetivo. Al examinar cualquier categoría por ejemplo, la eficacia y eficiencia de las operaciones, los cinco componentes han de estar presente y funcionando de forma apropiada para poder concluir que el control interno sobre las operaciones es eficaz.

Si se examina la categoría relacionada con los controles sobre la información financiera, por ejemplo, se deben cumplir los cinco criterios para poder concluir que el control interno de la información financiera es eficaz.

3.3.4.4. Aportación de Cada Componente

3.3.4.4.1. Entorno de Control

El entorno de control marca la pauta del funcionamiento de una empresa e influye en la concienciación de sus empleados respecto al control. Es la base de todos los demás componentes del control interno, aportando disciplina y estructura. Los factores del entorno de control incluyen la integridad, los valores éticos y la capacidad de los empleados de la empresa, la filosofía de dirección y el estilo de gestión, la manera en que la dirección asigna autoridad y las responsabilidades y organiza y desarrolla profesionalmente a sus empleados y la atención y orientación que proporciona al consejo de administración.

"El núcleo de un negocio es su personal (sus atributos individuales, incluyendo la integridad, los valores éticos y la profesionalidad) y el entorno en que trabaja, los empleados son el motor que impulsa la entidad y los cimientos sobre los que descansa todo".

El Entorno de control propicia la estructura en la que se deben cumplir los objetivos y la preparación del hombre que hará que se cumplan.

3.3.4.4.2. **EVALUACIÓN DE LOS RIESGOS**

Las organizaciones, cualquiera sea su tamaño, se enfrentan a diversos riesgos de origen externos e internos que tienen que ser evaluados. Una condición previa a la evaluación del riesgo es la identificación de los objetivos a los distintos niveles, vinculados entre sí e internamente coherentes. La evaluación de los riesgos consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo han de ser gestionados los riesgos. Debido a que las condiciones económicas, industriales, legislativas y operativas continuarán cambiando continuamente, es necesario disponer de mecanismos para identificar y afrontar los riesgos asociados con el cambio.

"La entidad debe conocer y abordar los riesgos con que se enfrenta, estableciendo mecanismos para identificar, analizar y tratar los riesgos correspondientes en las distintas áreas".
Aunque para crecer es necesario asumir riesgos prudentes, la dirección debe identificar y analizar riesgos, cuantificarlos, y prever la probabilidad de que ocurran así como las posibles consecuencias.

La evaluación del riesgo no es una tarea a cumplir de una vez para siempre. Debe ser un proceso continuo, una actividad básica de la organización, como la evaluación continua de la utilización de los sistemas de información o la mejora continua de los procesos.

Los procesos de evaluación del riesgo deben estar orientados al futuro, permitiendo a la dirección anticipar los nuevos riesgos y adoptar las medidas oportunas para minimizar y/o eliminar el impacto de los mismos en el logro de los resultados esperados. La evaluación del riesgo tiene un carácter preventivo y se debe convertir en parte natural del proceso de planificación de la empresa.

3.3.4.4.3. **Actividades de Control**

Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que se lleven a cabo las instrucciones de la dirección de la empresa. Ayudan a asegurar que se tomen las medidas necesarias para controlar los riesgos relacionados con la consecución de los objetivos de la empresa. Hay actividades de control en toda la organización, a todos los niveles y en todas las funciones.

Las actividades de control existen a través de toda la organización y se dan en toda la organización, a todos los niveles y en todas las funciones, e incluyen cosas tales como; aprobaciones, autorizaciones, verificaciones, conciliaciones, análisis de la eficacia operativa,

seguridad de los activos, y segregación de funciones.

En algunos entornos, las actividades de control se clasifican en; controles preventivos, controles de detección, controles correctivos, controles manuales o de usuario, controles informáticos o de tecnología de información, y controles de la dirección. Independientemente de la clasificación que se adopte, las actividades de control deben ser adecuadas para los riesgos.

Hay muchas posibilidades diferentes en lo relativo a actividades concretas de control, lo importante es que se combinen para formar una estructura coherente de control global.

Las empresas pueden llegar a padecer un exceso de controles hasta el punto que las actividades de control les impidan operar de manera eficiente, lo que disminuye la calidad del sistema de control. Por ejemplo, un proceso de aprobación que requiera firmas diferentes puede no ser tan eficaz como un proceso que requiera una o dos firmas autorizadas de funcionarios componentes que realmente verifiquen lo que están aprobando antes de estampar su firma. Un gran número de actividades de control o de personas que participan en ellas no asegura necesariamente la calidad del sistema de control.

3.3.4.4.4. **Información y Comunicación**

Se debe identificar, recopilar y comunicar información pertinente en forma y plazo que permitan cumplir a cada empleado con sus responsabilidades. Los sistemas informáticos producen informes que contienen información operativa, financiera y datos sobre el cumplimiento de las normas que permite dirigir y controlar el negocio de forma adecuada.

Dichos sistemas no sólo manejan datos generados internamente, sino también información sobre acontecimientos internos, actividades y condiciones relevantes para la toma de decisiones de gestión así como para la presentación de información a terceros. También debe haber una comunicación eficaz en un sentido más amplio, que fluya en todas las direcciones a través de todos los ámbitos de la organización, de arriba hacia abajo y a la inversa.

El mensaje por parte de la alta dirección a todo el personal ha de ser claro; las responsabilidades del control han de tomarse en serio. Los empleados tienen que comprender cuál es el papel en el sistema de control interno y como las actividades individuales estén relacionadas con el trabajo de los demás. Por otra parte, han de tener medios para comunicar la información significativa a los niveles superiores. Asimismo, tiene que haber una comunicación eficaz con terceros, como clientes, proveedores, organismos de control y accionistas.

En la actualidad nadie concibe la gestión de una empresa sin sistemas de información. La tecnología de información se ha convertido en algo tan corriente que se da por descontada. En muchas organizaciones los directores se quejan de que los voluminosos informes que reciben les exigen revisar demasiados datos para extraer la información pertinente.

En tales casos puede haber comunicación pero la información está presentada de manera que el individuo no la puede utilizar o no la utiliza real y efectivamente. Para ser verdaderamente efectiva la TI debe estar integrada en las operaciones de manera que soporte estrategias proactivas en lugar de reactivas.

Todo el personal, especialmente el que cumple importantes funciones operativas o financieras, debe recibir y entender el mensaje de la alta dirección, de que las obligaciones en materia de control deben tomare en serio. Asimismo debe conocer su propio papel en el sistema de control interno, así como la forma en que sus actividades individuales se relacionan con el trabajo de los demás.

Si no se conoce el sistema de control, los cometidos específicos y las obligaciones en el sistema, es probable que surjan problemas. Los empleados también deben conocer cómo sus actividades se relacionan con el trabajo de los demás.

Debe existir una comunicación efectiva a través de toda la organización. El libre flujo de ideas y el intercambio de información son vitales. La comunicación en sentido ascendente es con frecuencia la más difícil, especialmente en las organizaciones grandes. Sin embargo, es evidente la importancia que tiene.

Los empleados que trabajan en la primera línea cumpliendo delicadas funciones operativas e interactúan directamente con el público y las autoridades, son a menudo los mejor situados para reconocer y comunicar los problemas a medida que surgen.

El fomentar un ambiente adecuado para promover una comunicación abierta y efectiva está fuera del alcance de los manuales de políticas y procedimientos. Depende del ambiente que reina en la organización y del tono que da la alta dirección.

Los empleados deben saber que sus superiores desean enterarse de los problemas, y que no se limitarán a apoyar la idea y después adoptarán medidas contra los empleados que saquen a luz cosas negativas. En empresas o departamentos mal gestionados se busca la correspondiente información pero no se adoptan medidas y la persona que proporciona la información puede sufrir

las consecuencias.

Además de la comunicación interna debe existir una comunicación efectiva con entidades externas tales como accionistas, autoridades, proveedores y clientes. Ello contribuye a que las entidades correspondientes comprendan lo que ocurre dentro de la organización y se mantengan bien informadas. Por otra parte, la información comunicada por entidades externas a menudo contiene datos importantes sobre el sistema de control interno.

3.3.4.4.5. **Supervisión y Monitoreo**

Los sistemas de control interno requieren supervisión, es decir, un proceso que comprueba que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continuada, evaluaciones periódicas o una combinación de ambas cosas. La supervisión continuada se da en el transcurso de las operaciones. Incluye tanto las actividades normales de dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones. El alcance y la frecuencia de las evaluaciones periódicas dependerán esencialmente de una evaluación de los riesgos y de la eficacia de los procesos de supervisión continuada. Las deficiencias detectadas en el control interno deberán ser notificadas a niveles superiores, mientras que la alta dirección y el consejo de administración deberán ser informados de los aspectos significativos observados.

"Todo el proceso debe ser supervisado, introduciéndose las modificaciones pertinentes cuando se estime necesario. De esta forma el sistema puede reaccionar ágilmente y cambiar de acuerdo a las circunstancias".

Es preciso supervisar continuamente los controles internos para asegurarse de que el proceso funciona según lo previsto. Esto es muy importante porque a medida que cambian los factores internos y externos, controles que una vez resultaron idóneos y efectivos pueden dejar de ser adecuados y de dar a la dirección la razonable seguridad que ofrecían antes.

El alcance y frecuencia de las actividades de supervisión dependen de los riesgos a controlar y del grado de confianza que inspira a la dirección el proceso de control. La supervisión de los controles internos puede realizarse mediante actividades continuas incorporadas a los procesos empresariales y mediante evaluaciones separadas por parte de la dirección, de la función de auditoria interna o de personas independientes. Las actividades de supervisión continua destinadas a comprobar la eficacia de los controles internos incluyen las actividades periódicas de dirección y supervisión, comparaciones, conciliaciones, y otras acciones de rutina.

Luego del análisis de cada uno de los componentes, podemos sintetizar que éstos, vinculados entre sí:

- ✓ Generan una sinergia y forman un sistema integrado que responde de una manera dinámica a las circunstancias cambiantes del entorno.
- ✓ Son influidos e influyen en los métodos y estilos de dirección aplicables en las empresas e inciden directamente en el sistema de gestión, teniendo como premisa que el hombre es el activo más importante de toda organización y necesita tener una participación más activa en el proceso de dirección y sentirse parte integrante del Sistema de Control Interno que se aplique.
- ✓ Están entrelazados con las actividades operativas de la entidad coadyuvando a la eficiencia y eficacia de las mismas.
- ✓ Permiten mantener el control sobre todas las actividades.

- ✓ Su funcionamiento eficaz proporciona un grado de seguridad razonable de que una o más de las categorías de objetivos establecidas van a cumplirse. Por consiguiente, estos componentes también son criterios para determinar si el control interno es eficaz.
- ✓ Marcan una diferencia con el enfoque tradicional de control interno dirigido al área financiera.
- ✓ Coadyuvan al cumplimiento de los objetivos organizacionales en sentido general.

CAPITULO IV

4. LEY SARBANES OXLEY

4.1. RESEÑA HISTÓRICA

La Ley Sarbanes-Oxley es una Ley federal de Estados Unidos que ha generado una gran controversia, y que supuso la respuesta a los escándalos financieros de algunas grandes corporaciones, como los de Enron, Tyco International, WorldCom y Peregrine Systems.

Estos escándalos hicieron caer la confianza de la opinión pública en las empresas de auditoría y contabilidad. La Ley toma su nombre del senador del partido demócrata Paul Sarbanes y el congresista del partido republicano Michael G. Oxley.

Fue aprobada por amplia mayoría, tanto en el congreso como el senado y abarca y establece nuevos estándares de actuación para los consejos de administración y dirección de las sociedades así como los mecanismos contables de todas las empresas que cotizan en bolsa en Estados Unidos.

Introduce también responsabilidades penales para los consejos de administración y unos requerimientos por parte de la SEC (Securities and Exchanges Commission), organismo encargado de regulación del mercado de valores de Estados Unidos. Los partidarios de esta Ley afirman que la legislación era necesaria y útil, mientras los críticos creen que causará más daño económico del que previene.

La primera y más importante parte de la Ley establece una nueva agencia privada sin ánimo de lucro, “the Public Company Accounting Oversight Board", es decir, una compañía reguladora encargada de revisar, regular, inspeccionar y sancionar a las empresas de auditoría. La Ley también se refiere a la independencia de las auditoras, el gobierno corporativo y la transparencia financiera. Se considera uno de los cambios más significativos en la legislación empresarial, desde el *New Deal* de 1930.

A continuación se detallan los orígenes de la ley:

- A finales de la década del noventa, un conjunto de escándalos contables y financieros impactó en los mercados de capitales (Enron, WorldComm)
- Inversores empiezan a dudar sobre la veracidad de la información que se exponía en los estados contables.
- Es una condición indispensable que la información de que se dispone sea confiable, la

violación o perdida de este principio hace prácticamente inviable la existencia de un mercado de capitales.

- Ante este descrédito, fue necesario elaborar un marco legal que volviera a reinstaurar la confianza de los inversores en la autenticidad de la información que las empresas difundían en materia contable.

4.2. UN BREVE RESUMEN DE LA LEY

La "Ley de Reforma de la Contabilidad de Compañías Públicas y Protección de los Inversionistas" denominada la ley Sarbanes Oxley posee la siguiente estructura:

- Título I: Junta de Supervisión de Firmas de Contabilidad Pública
- Título II: Independencia de los Auditores
- Título III: Responsabilidad Corporativa
- Título IV: Revelaciones Financiera Mejoradas
- Título V: Conflicto de Intereses de los Analistas
- Título VI: Recursos y Autoridad de la Comisión
- Título VII: Estudios e Informes
- Título VIII y XI: Responsabilidad Corporativa y Fraude Criminal; Fraude y Responsabilidad Corporativa
- Título IX: Mejoramiento de Sanciones por Crímenes de "Cuello y Corbata"
- Título X: Declaraciones de Impuestos Corporativas

Quizás lo más relevante o lo distinto y nuevo que aporta esta normativa tienen relación a los títulos III y IV y en particular las secciones 302 y 404 que tienen relación a los controles internos, el status de estas dos secciones en las compañías es lo que este estudio pretende develar, de todas formas a continuación se presenta un breve resumen de algunos títulos y de lo que representan.

Y por supuesto nos referiremos a fondo sobre las secciones antes mencionada.

Título I: Junta de Supervisión de Firmas de Contabilidad Pública (Public Company Accounting Oversight Board "PCAOB"): Refuerza el cumplimiento de las anteriores leyes, normando además en las reglas de la junta, las normas profesionales y las leyes de valores relacionadas con la preparación y emisión de los informes de auditoría además de definir las correspondientes obligaciones de los auditores. Se Imponen sanciones por las violaciones a estas normas (principalmente monetaria).

Título II: Independencia de los Auditores, Servicios fuera del alcance de la auditoria: La compañía auditada no puede recibir de su mismo auditor, servicios profesionales como: Servicios de contabilidad, servicios de nómina,búsqueda de ejecutivos para contratación, preparación de informes sobre proyecciones y valuaciones, otorgar consejería legal (actuar como asesor en el área impositiva o laboral si es permitido) y realizar auditorías internas ni Intermediación financiera.

Títulos III y IV, Estructuras y Principales Impactos: A pesar de la existencia de numerosas secciones, las que tienen un mayor efecto en las empresas que cotizan en la Bolsa de Valores de Estados Unidos y sus subsidiarias son las Secciones 302 del Título III sobre Responsabilidad Corporativa por Informes Financieros y 404 del Título IV sobre Evaluación Gerencial de los Controles Internos.

- **Título III:** La administración debe implantar controles internos y procedimientos que aseguren que la información financiera es procesada, registrada y revelada de acuerdo a la normativa de la SEC. Estos controles reciben el nombre de "Controles y Procedimientos de Revelación". Por su parte el CEO y el CFO de cada compañía son responsables de, primero, establecer y mantener los "Controles y Procedimientos de Revelación". Segundo, diseñar dichos Controles de manera que aseguren que la información importante sea revelada para el período en que emiten el informe. Tercero, evaluar la eficacia de los "Controles y Procedimientos de Revelación". Y Cuarto, presentar en su informe las conclusiones respecto a la eficacia de los "Controles y Procedimientos de Revelación" basado en su propia evaluación, es decir sus conclusiones personales y no de la compañía. Estos informes son anuales y semestrales deben certificar que tanto el CEO y CFO han:

  - Revisado que los Estados Financieros no contienen declaraciones falsas de hechos materiales ni omisiones, y que además representan adecuadamente, en todos los aspectos materiales, la situación financiera y los resultados operacionales reales de la compañía.
  - Revelado a los auditores y al comité de auditoría todas las deficiencias significativas en el control interno y cualquier fraude.
  - Además, deben expresar formalmente que son ellos los responsables, de establecer y mantener controles internos, y que han revelado a los auditores y al comité de auditoría todas las deficiencias significativas en el control interno y cualquier fraude que pudiese haber existido.

- **Título IV:** En particular, la sección 404 requiere bastante tiempo, personas y recursos, por cuanto se debe develar y analizar todos los procedimientos de los procesos internos de las

compañías, además de encontrar, reconocer y en algunos casos crear controles internos para cada proceso.

Los Auditores Externos deben emitir también una opinión sobre el control interno, este informe debe señalar la responsabilidad de la administración de establecer y mantener una estructura y procedimientos adecuados de control interno para informes financieros.

Además debe incluir una evaluación de la efectividad de la estructura y procedimientos de control interno del emisor para los informes financieros. Cada memoria anual debe incluir un informe de la gerencia en el que se evalúen estos controles internos, mientras los auditores externos deben certificar esta evaluación que ha hecho la gerencia de la compañía y debe informar dichos resultados.

4.3. EL CASO ENRON.

Este caso marca un hito muy importante en los EEUU pues para muchos el desastre ocasionado por Enron fue tan grande que es comparable con el de las Torres Gemelas ocurrido meses antes de que estallara todo. Enron, era una pequeña compañía de gas que creció rápidamente y expandió sus negocios hacia otros rubros insospechados y nuevos hasta tener presencia en cerca de 40 países, lo cual la hacía ver como una empresa innovadora y sólida ante los ojos de todos.

Las personas la admiraban, las compañías querían ser como ella y también marcar diferencia porque eso es lo que vendía Enron, diferenciación, lo cual le ayudó a tener una imagen de empresa estable y en crecimiento. Nadie dudaba de ella, incluidos los auditores y sus empleados, quienes invertían el dinero de toda su vida en la que sería la inversión del millón, sin saber la realidad de los hechos.

La verdad era que Enron no era la empresa que se había encargado de pregonar, estaba teniendo muchas pérdidas e incurría en robos financieros que eran ocultados por los ejecutivos de alto mando. No obstante, esto no se sabría sino hasta mucho después cuando la extrañeza sobre sus siempre crecientes ganancias empezó a acrecentarse y la presión terminó por hacer que los ejecutivos de Enron revelen su real situación.

Antecedentes

Enron empezó como una pequeña empresa proveedora de gas en 1985 en Texas llamada Houston Natural Gas Company (HNG) pero debido a factores como la caída de la demanda del gas natural y la liberación de las regulaciones para su transporte, tuvo que fusionarse con otras empresas para no

desaparecer y por el contrario asentarse mejor en el mercado y así fue pues su fundador Ken Lay tenía una visión muy clara, que Enron creciera rápido y ganara dinero mientras seguía creciendo. Mientras tanto, Lay se había convertido en EEUU en una especie de precursor empresarial reconocido por sus ideas sobre la desregulación, lo cual lo llevó inicialmente a hacerle oposición al gobierno. No obstante, debido a su creciente popularidad y a intereses políticos y económicos tanto de EEUU como de Lay, éste llegó a tener un puesto no oficial en el gobierno como Embajador de las Desregulaciones. Para entonces, el ya presidente electo W. Bush mantenía una muy buena relación amical con Lay pues éste había financiado más que gran parte de su campaña política, razón por la cual Bush le otorgó muchos beneficios a Enron como la obtención de subsidios para la empresa. Lo cual obviamente dejaba ver el gran poder político que poseía Enron.(GIBNEY, n.d.)

Lay y el escándalo aceitoso: Vahalla

Lay tenía un objetivo claro, generar cuantiosas ganancias sin importar el costo. Fue entonces que Borget y Mastroeni, dos corredores de la empresa Enron Oil Co de la corporación Enron que se dedicaban a comprar y vender la energía como si se estuviera en un mercado de futuros no dejaban de ganar dinero. Para Lay, ellos eran la solución para las pérdidas que venían afrontando y no pensaba "perder la gallinita de los huevos de oro" más bien por el contrario los animaba a jugar y seguir apostando más, a pesar de que el banco Standard Chartered Bank ya le había informado de las irregularidades observadas en sus transacciones como el auto envío de dinero de un banco a otro. No obstante, no fue sino hasta que se probaron sus delitos por el desfalco a la empresa que fueron encarcelados. (BETANCOURT, n.d.)

La ideología Skilling y su valor hipotético a futuro

El fundador de Enron sabía que debía conseguir un reemplazo para ambos corredores y encontrar un medio para seguirle generando dinero a la empresa. Con este anhelo contrató a Jeff Skilling, que encontró una nueva forma de entregar energía, transformándola en instrumentos financieron que pudieran ser comercializados como acciones y bonos. Pronto Skilling, quien era un visionario, difundió en Enron la promesa de estabilidad, crecimiento, innovación y la existencia de un mundo nuevo.

Él era el exitoso líder respetado y querido por todos que hacía que las cosas sucediesen no obstante fue el causante del primer gran engranaje de la caída de Enron, manejar su contabilidad como "valor-hipotético-a-futuro". El cual consistía en anotar todas las ganancias que se han proyectado tener en el futuro sin importar si el dinero ya entró a la empresa o todavía, o si se estaban teniendo pérdidas.

Con ello se violaban principios básicos de la contabilidad como realización (porque no se reconocen los hechos económicos que pasan) y prudencia (porque se sobreestiman los activos y los ingresos). Ésta forma de manejar la contabilidad era subjetiva y manipuladora, además de irrealista y no permitía tomar decisiones acertadas.

Jeff asimismo implementó el "Comité de Revisión de Desempeño" que implicaba calificar a los empleados en una escala del 1 al 5 y despedir al 10% de ellos, según él, para incrementar la productividad en la empresa, sin ningún criterio con sustento.

Lo cual visto desde un punto de vista ético y también del de los negocios no es correcto ni rentable pues no motiva al empleado a trabajar en un buen clima laboral y se viola su derecho a tener estabilidad de contrato y a no tener un despido arbitrario.

Situación Legal

En Mayo del 2004, más de 20 mil ex empleados ganaron una demanda frente a Enron por $ 85 millones de dólares para tratar de compensar los cerca de $ 2 mil millones que habían perdido concepto de sus planes de ahorro dentro de la compañía y jubilación. Al año siguiente, algunos ex inversionistas recibieron otro monto por $ 4.2 millones de dólares.

Dos años después, el 25 de Mayo del 2006 fueron declarados culpables de los cargos de conspiración y fraude el ex presidente de la compañía, Kenneth Lay y su ex director ejecutivo, Jeffrey Skilling. El 5 de Julio del mismo año, Kenneth Lay, quien se enfrentaba a una posible condena de 45 años de cárcel fallece producto de problemas coronarios. Por su parte, Jeffrey Skilling es condenado a una pena de 24 años en prisión el 23 de Octubre de la fecha del juicio.
Finalmente, en Septiembre del año 2008, se acordó restituir a los ex accionistas un monto de $ 7.2 mil millones de dólares americanos a partir de una demanda fundada por un total de $ 40 mil millones de dólares por el concepto de pérdidas acarreadas debido a los sucesos del caso Enron.

4.4. NOVEDADES Y PUNTOS MÁS IMPORTANTES QUE INTRODUCELA LEYSARBANES-OXLEY.

- La creación del Public Company Accounting Oversight Board (Comisión encargada de supervisar las auditorías de las compañías que cotizan en bolsa).
- El requerimiento de que las compañías que cotizan en bolsa garanticen la veracidad de las evaluaciones de sus controles internos en el informe financiero, así como que los auditores independientes de estas compañías constaten esta transparencia y veracidad.

- Certificación de los informes financieros, por parte del comité ejecutivo y financiero de la empresa.
- Independencia de la empresa auditora.
- El requerimiento de que las compañías que cotizan en bolsa tengan un comité de auditoría, con consejeros completamente independientes, que supervisen la relación entre la compañía y sus auditores externos. Este comité de auditoría pertenece al consejo de administración, y los miembros que lo forman son completamente independientes a la misma. Esto implica que sobre los miembros, que forman el comité de auditoría, recae la responsabilidad de confirmar la independencia.
- Prohibición de préstamos personales a directores y ejecutivos.
- Transparencia de la información de acciones y opciones, de la compañía en cuestión, que puedan tener los directivos, ejecutivos y empleados claves de la compañía y consorcios, en el caso de que posean más de un 10 % de acciones de la compañía. Asimismo estos datos deben estar reflejados en los informes de las compañías.
- Endurecimiento de la responsabilidad civil, así como las penas, ante el incumplimiento de la Ley. Se alargan las penas de prisión, así como las multas a los altos ejecutivos que incumplen y/o permiten el incumplimiento de las exigencias en lo referente al informe financiero.
- Protecciones a los empleados en el caso de fraude corporativo. La OSHA (Oficina de Empleo y Salud) se encargará en menos de 90 días de reinsertar al trabajador, se establece una indemnización por daños, la devolución del dinero defraudado, los gastos en pleitos legales y otros costes.

4.4.1. Requerimientos que establece la PCAOB en relación al Artículo404

- Asesoramiento del diseño y la eficacia del funcionamiento del os controles internos relacionados con el mantenimiento de los balances financieros relevantes.
- Comprensión de la importancia de las transacciones anotadas, autorizadas, procesadas, y contabilizadas.
- Documentar suficiente información sobre el flujo de transacciones para identificar posibles errores o fraudes que hayan podido ocurrir.
- Evaluar la credibilidad de los controles de la compañía, de acuerdo con el "COSO" (Committee of Sponsoring Organizations of theTreadway Commission), organización encargada de identificar fraudes financieros.
- Evaluar los controles diseñados para prevenir o detectar fraudes, incluidos los controles a la dirección.

- Evaluar el control del proceso del informe financiero al final de ejercicio.
- Evaluar el control sobre la veracidad de los asientos contables.

4.5. CONTROLES INTERNOS

4.5.1. Sección302

Los artículos referentes a controles internos, son quizás los más importantes de la Ley.

En el artículo 302 de la Ley se establecen los procedimientos internos con el fin de asegurar la transparencia financiera.

También se específica la responsabilidad penal que recae sobre los directivos de las empresas, ya que tienen que firmar unos informes de forma que aseguren la veracidad de los datos que estos contienen. Los funcionarios firmantes certifican que ellos son responsables.

Esto es un cambio sustancial en lo referente a la legislación pasada, ya que al menos hay una persona que firma y, ante posibles irregularidades o fraudes, esta persona firmante será la responsable.

Con esto, a la auditora externa se le exime de culpa, o al menos de parte de culpa, ya que el informe de auditoría se efectúa a partir de los informes que le concede la compañía.

Si el informe que le es entregado a la empresa auditora está mal diseñado, contiene información falsa o está falto de información, la responsabilidad recae sobre el ejecutivo de la compañía auditada que ha firmado los informes. Esto otorga una independencia declarada y comprobada de la empresa auditora con respecto a la compañía a auditar.

La Ley Sarbanes-Oxley establece un responsable o responsables, una cabeza de turco sobre la que recaerán las posibles consecuencias ante un fraude; algo que anteriormente no existía y que conllevaba dificultades legales a la hora de buscar responsables, como ocurrió en el caso Enron. En este caso fueron imputados varios de los directivos, y finalmente todos menos dos quedaron absueltos. ((Sarbanes-Oxley Act, n.d.)

4.6. RESPONSABILIDAD DE LA COMPAÑÍA POR LOS INFORMES FINANCIEROS.

4.6.1. Reglamentos requeridos.

La comisión, por reglamento, requerirá de cada compañía que presente informes periódicos.
Que el principal funcionario o funcionarios ejecutivos y el principal funcionario o funcionarios financieros, o personas que efectúen funciones similares, en cada informe anual o trimestral, presentado o suministrado bajo cualquier artículo de tal ley certifique que:

1. El funcionario firmante ha revisado el informe.

2. El informe no contiene ninguna declaración falsa de un hecho material u omite declarar un hecho material necesario a fin de hacer que a luz de las circunstancias bajo las cuales fueron hechos tales informes no son fraudulentos.

3. Los estados financieros, y otra información incluida en el informe presentan razonablemente la situación financiera y los resultados de las operaciones del emisor por los períodos presentados en el informe.

4. Los funcionarios firmantes:
    a. Son responsables por establecer y mantener controles internos.
    b. Han diseñado controles internos para asegurar que información importante referente al emisor sea puesto en conocimiento de tales funcionarios.

5. Los funcionarios firmantes han revelado a los auditores del emisor y al comité de auditoría de la junta de directores (o personas que desempeñan función equivalente)
    a. Todas las deficiencias de los controles internos que podrían afectar adversamente la habilidad del emisor para registrar, procesar, resumir y reportar datos financieros.
    b. Cualquier fraude, significativo o no, que involucre a la gerencia u otros empleados que desempeñen un papel importante en los controles internos del emisor.

4.7. ARTÍCULO (404) LEY SARBANESOXLEY

La novedad que introduce el artículo 404 de la Ley SARBANES-OXLEY es la exigencia de redactar un informe de control interno al final de cada ejercicio fiscal.

Dentro de este informe de control interno se establece la responsabilidad del equipo directivo de tener una estructura de control interno adecuada. Anteriormente esta exigencia no existía y ahora el equipo directivo es responsable ante posibles fraudes.

Por ejemplo, en el caso Enron no existía control interno declarado y los movimientos de ingeniería financiera entre filiales de Enron en paraísos fiscales y la central en EEUU quedaban sin ser vigilados ni controlados, de lo cual un caso extremo fue lo ocurrido en el año 2001 anteriormente mencionado.

Este informe de control interno es revisado y evaluado por la empresa auditora, que certificara la anterior evaluación hecha por la comisión de los directivos encargados de realizar dicho informe.

4.7.1. EVALUACION DE LA GERENCIA DE LOS CONTROLESINTERNOS.

4.7.1.1. Regulaciones Requeridas.

La Comisión prescribirá regulaciones requiriendo que cada informe anual contenga un informe de control interno, el cual:

1. Determinará la responsabilidad de la gerencia por establecer y mantener una estructura adecuada de control interno y los procedimientos.
2. Contendrá una evaluación, al final del año fiscal más reciente del emisor, de la estructura de control interno y los procedimientos para la información financiera.

4.7.1.2. Evaluación e informe del control interno.

Con respecto a la evaluación del control interno requerido por el inciso (a), cada firma de contabilidad pública que prepara o emite el informe de auditoría para el emisor testificará e informará sobre la evaluación hecha por la gerencia de emisor.
Una testificación bajo esta subsección será hecha de acuerdo con las normas para compromisos de testificación emitidas o adoptadas por la Junta. La testificación no estará sujeta a un compromiso separado.

4.8. ARTÍCULO (906) LEY SARBANES OXLEY

La Ley establece una modificación en el código penal de los Estados Unidos. El artículo906 de la Ley Sarbanes Oxley establece una nueva disposición en el código penal donde se especifican las

multas y penas para los responsables legales de infracción de los requerimientos expuestos en la Ley SARBANES- OXLEY.

El responsable "será multado con no más de 1.000.000 $ o encarcelado porno más de 10 años, o ambos" en el caso de certificar el informe periódico sabiendo que no cumple con todos los requerimientos de la ley".

El responsable "será multado con no más de 5.000.000 $ o encarcelado porno más de 20 años, o ambos" en el caso de certificar el informe periódico intencionadamente sabiendo que no cumple con todos los requerimientos de la ley".

Esta sección del código penal que ha introducido la Ley Sarbanes Oxley es toda una novedad, porque específica la pena del tipo de delito financiero en cuestión, y endurece las penas anteriormente existentes para este tipo de delitos.

Además de especificar la pena, también aclara sobre quién recae la responsabilidad, a diferencia de lo ocurrido con el caso de los escándalos de Enron y otras compañías donde la responsabilidad penal no fue fácil de establecer en unos culpables claros.

4.9. COSTE DE IMPLEMENTACIÓN.

Existen distintas opiniones acerca de la Ley, John Thain (NYSE Chief Executive Officer) establece "No hay lugar a dudas que la Ley SARBANES-OXLEY era necesaria". No obstante, el coste de implementación de los nuevos requerimientos ha llevado a las compañías a cuestionarse la necesidad de la Ley.

Para las compañías, la necesidad de actualizar los sistemas de información para cumplir los requerimientos de control e informe suponen un gran coste. En muchos de los casos esto implica cambios significativos o incluso reemplazarlos, ya que anteriormente fueron diseñados sin la necesidad del cumplimiento de los nuevos estamentos. Recientemente artículos publicados en el New York Times, Wall Street Journal, Financial Times y The Economist han sugerido que las opiniones de la Ley SARBANES-OXLEY son la causa de un decrecimiento de las compañías americanas cotizadas en bolsa en comparación con otras bolsa como Londres o Hong Kong, es decir, la Ley desincentiva a las compañías para cotizar en bolsas americanas.

Se ha comprobado que el coste asociado al cumplimiento del apartado 404 de la Ley SARBANES-OXLEY es realmente significativo. Según "Financial Executives International" (FEI), en una

muestra de 217 compañías con un promedio de ingresos mayores de 5.000 millones de dólares, se estimó un coste de 4,36 millones de dólares en el primer año.

El gran coste de implementación incurrido durante el primer año, puede ser atribuido a la gran carga de trabajo que tuvieron que realizar las auditoras, y el coste monetario que esto acarrea. Estos costes de establecimiento de la Ley puede ser poco significantes para una minoría de grandes compañías, no obstante puede llegar a ser insostenible para una empresa más pequeña con una facturación de unos pocos millones.

Por otro lado la Ley todavía no es efectiva para las compañías pequeñas con un valor de menos de 75 millones de dólares en el mercado bursátil, y todavía no está claro lo que la Ley requerirá a las pequeñas compañías, cuando ésta se haga efecto.

Conforme más compañías y auditoras ganen experiencia con la Ley Sarbanes-Oxley, se prevé que los costes vayan disminuyendo. Los ingresos de las auditoras han crecido mucho desde que entró en vigor la Ley, aunque ya estaban creciendo antes de la imposición de la Ley como consecuencia de los escándalos financieros por los cuales las autoridades se vieron obligados a redactar la Ley.
Hay quien afirma que la Ley Sarbanes-Oxley ha hecho que muchos negocios se hayan trasladado de Nueva York a Londres, donde las autoridades reguladoras de los servicios financieros son más flexibles.

Hace ya más de 3 años que el congreso de los Estados Unidos impuso la Ley con la intención de recuperar la confianza de los inversores. En los últimos 2 años, el artículo 404 de la Ley Sarbanes-Oxley, anteriormente explicado, ha requerido que la gestión de gran cantidad de compañías que cotizan en bolsa y sus compañías auditoras independientes escriba un informe sobre los controles internos de las compañías. Esto es lo que ha hecho incrementar los costes de auditoría.

4.10. VALORACIÓN CRÍTICA

La Ley Sarbanes-Oxley se aprobó con el fin de evitar posibles escándalos como los ocurridos a Enron, WorldCom, y demás compañías que sufrieron algo parecido.

En Estados Unidos hubo un gran revuelo, así como un descontento general por parte de los inversores, ya que desconfiaban de las instituciones reguladoras y del Gobierno.

Para evitar esa caída de la confianza aprobaron esta Ley, ya que a efectos prácticos no evita que pueda volver a ocurrir algo así. Esta Ley no podría evitar que una compañía haga una contabilidad

fraudulenta como hizo Enron. Si la información que se les ofrece a las compañías auditoras es falsa, o incompleta, éstas compañías auditoras harán unos informes irreales e incompletos.

Lo que sí establece la Ley es una responsabilidad, ya que hay una persona encargada de firmar los informes y de garantizar a la compañía auditora que la información es veraz y completa.

La Ley Sarbanes-Oxley ha supuesto unos grandes costes para las compañías, a la vez que ha supuesto unos mayores ingresos para las empresas dedicadas a auditoría independiente.

Esto ha supuesto un desincentivo para algunas compañías que iban a entrar a formar parte en el parqué americano, y que han decidido trasladarse a otros mercados como el europeo y japonés donde existe una mayor flexibilidad.

4.11. CONCLUSIÓN

- ✓ La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.
- ✓ La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.
- ✓ La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).
- ✓ En la mayoría de empresas existe una constante preocupación por la presencia ocasional de fraudes, sin embargo, muchos de estos podrían prevenirse. En algunos países de América Latina, donde normalmente los salarios son bajos, las crisis recurrentes y las necesidades de los trabajadores no se ven del todo satisfechas; y si a esto agregamos fallas en el control interno y la falta de vigilancia adecuada en las operaciones, entonces las posibilidades desde sufrir un fraude son grandes.

BIBLIOGRAFÍA

- CONTRALORÍA GENERAL DEL ESTADO. Manual de Auditoría Gubernamental.
- O. RAY WHITTINGTON. Principios de Auditoría. Décimo Cuarta Edición.
- http://www.monografias.com/trabajos75/historia-internet/historia internet3.shtml
- http://es.slideshare.net/1401201014052012/auditoria-informatica-12- 15846870
- http://docs.google.com/View?id=dcwjqhp4_0hgb2j3fh
- http://www.nobosti.com/spip.php?article69
- www.isaca.org

GLOSARIO DE TÉRMINOS

ACTIVIDADES DE CONTROL: Según COSO, hace referencia a los controles que realmente existen para minimizar los riesgos que enfrenta la empresa.

ACEPTAR EL RIESGO: Es uno de los métodos más comunes de manejar el riesgo, es la decisión de aceptar las consecuencias de la ocurrencia del evento.

ACTIVOS: Según Magerit, son los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

ADMINISTRACIÓN DEL RIESGO: según David McNamee, es un proceso que asegura la sensibilidad para detectar el riesgo, la flexibilidad para responder al riesgo, y la capacidad de recursos para mitigar los riesgos.

ADQUISICIÓN E IMPLEMENTACIÓN: Dominio de COBIT el cual, para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

AGENCIA DE PROYECTOS DE INVESTIGACIÓN AVANZADOS DE DEFENSA (DARPA): Proveniente desunombreoriginalen ingles Defense Advanced Research Projects Agency, es una agencia del Departamento de Defensa de Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar. Fue creada en 1958 como consecuencia tecnológica de la llamada Guerra Fría, y del que surgieron, década después, los fundamentos de ARPANET, red que dio origen a Internet

ADVANCED RESEARCH PROJECTS AGENCY NETWORK (ARPANET): es la red de computadoras creada por encargo del Departamento de Defensa (DOD) de Estados Unidos para utilizarla como medio de comunicación entre los diferentes organismos nacionales estadounidenses.

AICPA: American Institute of Certified Public Accountants – Instituto Americano de Contadores Públicos Certificados.

AMBIENTE DE CONTROL: Según COSO, hace referencia a la cultura corporativa de control que debe existir en una organización.

AMENAZA: (1) Es un factor del medio ambiente externo que puede ocasionar una falla en el desempeño futuro de las organizaciones. (2) Según Magerit, se definen como los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Las Amenazas se pueden materializar y transformarse en agresiones.

ANALISIS DE CAMPO DE FUERZA: Es una técnica utilizada para lograr una perspectiva completa de las fuerzas en pro y en contra de un plan, de manera que una decisión puede ser tomada teniendo en cuenta todos los intereses. Ayuda a reducir el impacto de las fuerzas en oposición, y fortalecer las fuerzas soporte.

ANÁLISIS DOFA: Este tipo de análisis examina la interacción entre las características particulares de la organización y el medio ambiente en el cual se desenvuelve.

APLICACIONES: Recurso de TI en COBIT, definido como sistemas de aplicación; la suma de procedimientos manuales y programados.

APPLET: Bases de datos locales de aplicaciones en Internet.

ARBOLES DE DECISION: Herramientas de gran relevancia para la toma de decisiones basada en aspectos financieros o en situaciones que impliquen números, donde se debe tener en cuenta una gran cantidad de información. Básicamente su estructura permite contemplar y evaluar alternativas y las implicaciones de tomar esas decisiones, permitiendo visualizar los riesgos que pueden derivarse de algunas alternativas.

ADMINISTRACIÓN DEL RIESGO: según David McNamee, es un proceso que asegura la sensibilidad para detectar el riesgo, la flexibilidad para responder al riesgo, y la capacidad de recursos para mitigar los riesgos.

ADQUISICIÓN E IMPLEMENTACIÓN: Dominio de COBIT el cual, para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

AICPA: American Institute of Certified Public Accountants – Instituto Americano de Contadores Públicos Certificados.

AMBIENTE DE CONTROL: Según COSO, hace referencia a la cultura corporativa de control que debe existir en una organización.

AMENAZA: (1) Es un factor del medio ambiente externo que puede ocasionar una falla en el desempeño futuro de las organizaciones. (2) Según Magerit, se definen como los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Las Amenazas se pueden materializar y transformarse en agresiones.

ANALISIS DE CAMPO DE FUERZA: Es una técnica utilizada para lograr una perspectiva completa de las fuerzas en pro y en contra de un plan, de manera que una decisión puede ser tomada teniendo en cuenta todos los intereses. Ayuda a reducir el impacto de las fuerzas en oposición, y fortalecer las fuerzas soporte.

ANÁLISIS DOFA: Este tipo de análisis examina la interacción entre las características particulares de la organización y el medio ambiente en el cual se desenvuelve.

APLICACIONES: Recurso de TI en COBIT, definido como sistemas de aplicación; la suma de procedimientos manuales y programados.

APPLET: Bases de datos locales de aplicaciones en Internet.

ARBOLES DE DECISION: Herramientas de gran relevancia para la toma de decisiones basada en aspectos financieros o en situaciones que impliquen números, donde se debe tener en cuenta una gran cantidad de información. Básicamente su estructura permite contemplar y evaluar alternativas y las implicaciones de tomar esas decisiones, permitiendo visualizar los riesgos que pueden derivarse de algunas alternativas.

ARPANET son las siglas de: Advanced Research Projects Agency Network, es la red de computadoras creada por encargo del Departamento de Defensa (DOD) de Estados Unidos para utilizarla como medio de comunicación entre los diferentes organismos nacionales estadounidenses.

AUDITORÍA: es un examen, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

AUDITORÍA BASADA EN LOS RIESGOS (ABR): metodología que se está empezando a implementar como parte del cambio al nuevo paradigma. Esta metodología tiene en cuenta los objetivos organizacionales para la evaluación de los riesgos y dar en su informe las recomen decisiones pertinentes sobre la mejor forma de manejar dichos riesgos.

AUDITORÍA DE CUMPLIMIENTO: consiste en la comprobación o examen de las operaciones financieras, administrativas, económicas y de otra índole de una entidad para establecer que se han realizado conforme a las normas legales, estatutarias y de procedimientos que le son aplicables.

AUDITORÍA DE GESTION: Este tipo de auditoría se encarga de evaluar el grado de eficacia y eficiencia con que se manejan los recursos de la entidad, y el grado de eficacia y eficiencia con que se logran los objetivos organizacionales.

AUDITORIA DE LOS SISTEMAS DE INFORMACIÓN: Es definida como cualquier auditoria que abarque la revisión y evaluación de todos los aspectos de los sistemas automáticos de procesamiento de la información, incluyendo los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

AUDITORÍA DE PROTECCION DE DATOS: Examen practicado para verificar que los datos electrónicos que maneja la organización poseen las medidas de seguridad apropiadas para evitar su conocimiento masivo y su potencial modificación ya sea parcial o total por parte de terceros.

AUDITORÍA FINANCIERA: examen de las operaciones financieras llevadas a cabo por una entidad con el fin de evaluarlas y verificarlas con posterioridad a su ejecución para determinar la razonabilidad de las cifras contenidas en los estados financieros.

AUDITORÍA INTEGRAL: es una auditoría que, como su nombre lo indica, integra en una sola labor la práctica de las auditorías financiera, de cumplimiento, de gestión y de control interno.

AUDITORÍA INTERNA: La Auditoría Interna es una actividad de aseguramiento y de consultoría independiente y objetiva, diseñada para adicionar valor y mejorar las operaciones de una organización. La Auditoría Interna ayuda a la organización a lograr sus objetivos brindando un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de administración del riesgo, de control y de gobierno corporativo.

BASE DE DATOS O **BANCO DE DATOS:** Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido; una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. Actualmente, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital, siendo este un componente electrónico, y por ende se ha desarrollado y se ofrece un amplio rango de soluciones al problema del almacenamiento de datos.

BENCHMARKING: el proceso de medir las operaciones de una organización contra operaciones similares con el propósito de mejorar los procesos del negocio. Su propósito es mejorar los productos y procesos para satisfacer mejor las necesidades de los clientes. Es decir, mirar lo que han hecho con éxito otras empresas de la misma industria en cuanto administrar los riesgos, y realizar las mismas acciones; en caso que aquellas empresas no hayan tenido buenos resultados, tener en cuenta esas situaciones para mejorarlas o para no realizarlas.

CICA: Canadian Institute of Chartered Accountants – Instituto Canadiense de Contadores Certificados.

CICLO DEL CAMBIO: modelo desarrollado por David MacNamee para entender las fases de crecimiento de un sistema u organización. Este ciclo no es lineal ni circular, sino que presenta las características de una espiral. El ciclo del cambio presenta tres fases: formación, normalización y cumplimiento; separadas por límites críticos, llamados breakpoints.

COBIT: Informe emitido por la Information Systems Audit and Control Foundation, órganos dependientes de ISACA que muestra procedimientos de auditoría que se pueden efectuar sobre sistemas de información.

COCO: Acrónimo de **C**riteria **o**f **Co**ntrol, una iniciativa del Canadian Institute of Chartered Accountants (CICA) para proveer una estructura de control, para el fortalecimiento del control y del gobierno corporativo en una organización.

CÓDIGO CADBURY (Cadbury Code): Metodología desarrollada por el Comité de Informes Financieros del Institute of Chartered Accountants of England and Wales (ICAEW) como un informe de riesgo.

COMPARTIR EL RIESGO: es un caso especial de la transferencia del riesgo, es también una forma de retener el riesgo. Cuando los riesgos son compartidos, la posibilidad de pérdida es

transferida de un individuo al grupo; sin embargo, compartir el riesgo es también una forma de retenerlo en la cual el riesgo "transferido" al grupo es retenido junto con los riesgos de los demás miembros del grupo.

COMPROMISO: Para CoCo, es un grupo de criterios que proveen un sentido de la identidad y valores de la organización.

CONFIABILIDAD DE LA INFORMACIÓN: Criterio de información de COBIT que hace referencia a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

CONFIDENCIALIDAD: Criterio de información de COBIT que hace referencia a la protección de información sensible contra divulgación no autorizada.

CONTRALORIA: Organismo de control que vigila la gestión fiscal de la administración y de los particulares o entidades que manejen fondos o bienes de la Nación.

CONTROL INTERNO: sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las normas u objetivos previstos.

CONTROL: Según CoCo, son todos los elementos de una organización – incluyendo sus recursos, sistemas, procesos, cultura, estructura y tareas –, que tomados en conjunto respaldan a la gente en el logro de los objetivos de la organización.

CONTROLAR EL RIESGO: el riesgo se controla a través de la prevención por medio de la implementación de controles y su monitoreo constante. Esta es una técnica ideal para el manejo de los riesgos, y es la más utilizada

COSO: Metodología de control emitida por el **C**ommittee **O**f **S**ponsoring **O**rganizations of the Treadway Commission.

COSTO: Impacto sobre el precio que se pagaría si se presenta un riesgo determinado.

CSA: Acrónimo de **C**ontrol **S**elf-**A**ssessment (Auto-Evaluación de Control) y es definido por McNamee como "la involucración de la gerencia y el personal en la evaluación de los controles internos dentro de su grupo de trabajo".

CUMPLIMIENTO: Criterio de información de COBIT que hace referencia al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.

CURVA ESTRATÉGICA RIESGO/OPORTUNIDAD: modelo desarrollado por David McNamee para mostrar la relación entre los conceptos de riesgo y oportunidad. Muestra además los efectos que tiene el tiempo (corto, mediano y largo plazo) sobre estos dos conceptos.

EFECTIVIDAD: Criterio de información de COBIT que hace referencia a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

EFICACIA: Factor de evaluación de los procesos en que se mide el logro apropiado de los objetivos.

EFICIENCIA: (1) Factor de evaluación de los procesos en que se mide el manejo apropiado de los recursos. (2) Criterio de información de COBIT que hace referencia a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

ENTREGA Y SOPORTE: Dominio de COBIT que hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

EQUIDAD: Factor de evaluación de los procesos en que se mide la imparcialidad en el trato y la justicia natural.

ETICA: Factor de evaluación de los procesos en que se mide la solidez de los principios morales de la organización.

EVALUACIÓN DE RIESGOS: Según COSO, es el examen de factores internos y externos que impiden el logro de los objetivos organizacionales.

EVALUACIÓN HIPOTETICA DE RIESGOS: Evaluación de riesgos que se efectúa en la fase de planeación, que se basa en el análisis del diagrama de flujo y los aportes de los responsables del (los) proceso(s) estudiado(s).

EVALUACIÓN PRÁCTICA DE RIESGOS: Evaluación de riesgos que se efectúa en el trabajo de campo, en que confronta los riesgos observados con los factores de riesgos para determinar las causas que originan la ocurrencia de los riesgos observados.

EVALUACIÓN PRELIMINAR DE RIESGOS: Evaluación de riesgos que se efectúa en la fase de evaluación de los controles, que se basa en el análisis realizado en la evaluación hipotética de riesgos y el estudio de la fortaleza del sistema de Control Interno.

EVITAR EL RIESGO: el riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse con la acción que origine el riesgo.

ICAEW: Institute of Chartered Accountants of England and Wales – Instituto de Contadores Certificados en Inglaterra y Wales.

IIA: Institute of Internal Auditors – Instituto de Auditores Internos.

IMACS: Internal Management and Consulting Services – Servicios de Administración y Consulta Interna.

IMPACTO: Según Magerit se define como un daño producido a la organización por un posible incidente y es el resultado de la Agresión sobre el Activo, o visto de manera más dinámica, la diferencia en las estimaciones de los estados (de seguridad) obtenidas antes y después del evento.

INCERTIDUMBRE: según Emmet Vaughan, es una reacción psicológica a la ausencia de conocimiento acerca del futuro. Con base en la teoría de la probabilidad, se puede medir en un intervalo entre 0 y 1.

INFORMACIÓN Y COMUNICACIÓN: Según COSO, es el proceso de retroalimentación que debe existir dentro de la empresa y entre ésta y su medio ambiente.

INSTALACIONES: Recurso de TI en COBIT, definido como los recursos para alojar y dar soporte a los sistemas de información.

INTEGRIDAD: Criterio de información de COBIT que hace referencia a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

ISACA: Information Systems Audit and Control Asociation.

IT: Information Technology – Tecnología de Información.

MONITOREO Y APRENDIZAJE: Para CoCo, es un grupo de criterios que proveen un sentido de la evolución de la organización.

MONITOREO: (1) Según COSO, se refiere al seguimiento permanente que se debe hacer, por parte de la administración, para evaluar la efectividad del sistema de control interno. (2) Dominio de COBIT el cual evalúa regularmente todos los procesos a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

NLS: soporte de idioma nacional

PERSONAL: Recurso de TI en COBIT, definido como las habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

PROCESAMIENTO DE DATOS (PAD): Es la recolección y manipulación de elementos de datos para producir información significativa.
El procesamiento de datos trata de un subconjunto del procesamiento de la información, el cambio (procesamiento) de la información de cualquier manera detectable por un observador. El procesamiento de datos es distinto del procesamiento de textos, pues este último manipula textos nada más en lugar de los datos.

PROCEDIMIENTO DE VERIFICACIÓN INTERNA: método utilizado en el segundo paradigma. Es descrito por Jaime Hernández como un método que utilizó procedimientos de selectividad para asegurar que las pruebas de auditoría cubrieran los ítems más importantes del universo de las operaciones, dada la imposibilidad de revisar el gran volumen de transacciones. Este "Procedimiento de Verificación Interna" fue una primera aproximación a lo que hoy en día se conoce como Sistema de Control Interno.

RIESGO: es una medida de incertidumbre que refleja hechos presentes o futuros que pueden ocasionar una ruptura en el flujo de información o incumplimiento en el logro de los objetivos organizacionales.

RIESGO ABSOLUTO: El máximo riesgo sin los efectos mitigantes de controles internos.

RIESGO ADMINISTRADO: Los riesgos y consecuencias después de la aplicación del control interno.

RIESGO DE COMPETENCIA: Factor interno y/o externo que se deriva con el mercado, y su área comercial en la venta de productos o prestación de servicios, y está encaminado a determinar la oportunidad y la capacidad de competencia que tiene la organización en el medio. Incluye variables como: Portafolio de productos, calidad del producto, canales de distribución, investigación y desarrollo, servicio al cliente, entre otras.

RIESGO DE CONTROL: La tendencia del sistema de control interno de perder eficacia con el paso del tiempo y exponer, o no impedir la exposición de los activos que salvaguarda.

RIESGO DE DETECCIÓN: La probabilidad que se obtendrá una conclusión de auditoría errada a partir de los resultados de un examen.

RIESGO DE INFORMACIÓN: Son amenazas de uso de información de poca calidad para la toma de decisiones operacional, financiera o estratégica dentro del negocio y suministrar información distorsionada a terceras personas.

RIESGO DE PROCESO: (1) el riesgo proveniente de los procesos y productos clave utilizados para lograr las estrategias y los objetivos específicos de la unidad de negocio. (2) Es el riesgo sobre un proceso comercial.

RIESGO DE PROGRAMACIÓN: riesgos que incluyen la obtención y el uso de recursos y actividades aplicables que pueden estar por fuera del control del programa pero que pueden afectar la dirección del programa. Estos riesgos tienden a ser una función del ambiente del negocio.

RIESGO DE SOPORTE: riesgo asociado con los sistemas de mantenimiento y de operación que están siendo desarrollados y ejecutados actualmente.

RIESGO DINÁMICO: Los riesgos dinámicos son los que resultan de los cambios en la economía; surgen de dos tipos de factores: Factores en el medio externo, los cuales son incontrolables y los otros factores son las decisiones gerenciales dentro de la empresa.

RIESGO ESTÁTICO: Los riesgos estáticos involucran aquellas pérdidas que resultarían aun si no ocurren cambios en la economía.

RIESGO EXTERNO: resultan de circunstancias ajenas a la empresa que pueden ser difíciles o imposibles de controlar. Estos riesgos serían causados, en su mayoría, por fuerzas sociales, políticas o económicas.

RIESGO FINANCIERO: (1) Factor Interno que se relaciona directamente con el Capital de Trabajo, las fortalezas o debilidades financieras de la organización, en el manejo de sus finanzas, e incluye variables como: Liquidez, endeudamiento, margen de rentabilidad, rotación de activos corrientes y elasticidad en la demanda, entre otras. (2) se pueden considerar como parte de los riesgos internos y pueden ser resumidos como el riesgo que los flujos de caja no sean administrados efectivamente para: maximizar la disponibilidad del efectivo; para reducir incertidumbre en cuanto a la variación en la moneda, tasas de interés y créditos; y para mover fondos de efectivo de manera rápida y sin pérdida de valor a donde más se necesiten. Estos riesgos pueden tener un efecto directo en los activos y pasivos monetarios. (3) El riesgo financiero involucra la relación entre un individuo – o una organización – y un activo o un ingreso que se puede perder o dañar.

RIESGO INHERENTE: Es el que tiene que ver con la naturaleza propia de cada actividad.

RIESGO INTERNO: pueden ser "riesgo de proceso" o "riesgo de información para la toma de decisiones". Estos riesgos surgen dentro de una empresa como resultado de sus actividades de negocio. Generalmente, estos riesgos son más controlables que los riesgos externos.

RIESGO OPERATIVO: riesgo asociado con el ¿Qué tan bien operan los sistemas en cuanto a especificaciones de diseño o seguridad?

RIESGO TÉCNICO: Riesgo asociado con el desarrollo de un nuevo diseño para proveer un mayor nivel de desempeño que el previamente demostrado o el mismo o menor nivel de desempeño sujeto a nuevas restricciones. La naturaleza y causas de los riesgos técnicos son muy variadas, pero en general estos riesgos son el resultado de la demanda por un mayor desempeño de los nuevos sistemas y equipos.

RIESGO TECNOLÓGICO: Factor Interno y/o externo que incluye aspectos relacionados con el uso de tecnología tangible o intangible, infraestructura tecnológica, normalización de procesos, y la capacidad de reacción que tiene la organización en el uso de éstas.

SRI: Instituto de Investigación de Standford

TRANSMISSION CONTROL PROTOCOL **(TCP)** o **PROTOCOLO DE CONTROL DE TRANSMISIÓN:** Es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn.

Muchos programas dentro de una red de datos compuesta por redes de computadoras, pueden usar TCP para crear "conexiones" entre sí a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

TCP da soporte a muchas de las aplicaciones más populares de Internet (navegadores, intercambio de ficheros, clientes FTP, etc.) y protocolos de aplicación HTTP, SMTP, SSH y FTP.

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC): es un concepto que tiene dos significados. El término "tecnologías de la información" se usa a menudo para referirse a cualquier forma de hacer cómputo. Como nombre de un programa de licenciatura, se refiere a la preparación que tienen estudiantes para satisfacer las necesidades de tecnologías en cómputo y comunicación de gobiernos, seguridad social, escuelas y cualquier tipo de organización.

Planificar y gestionar la infraestructura de TIC de una organización es un trabajo difícil y complejo que requiere una base muy sólida de la aplicación de los conceptos fundamentales de áreas como las ciencias de la computación, así como de gestión y habilidades del personal. Se requieren habilidades especiales en la comprensión, por ejemplo de cómo se componen y se estructuran los sistemas en red, y cuáles son sus fortalezas y debilidades. En sistemas de información hay importantes preocupaciones de software como la fiabilidad, seguridad, facilidad de uso y la eficacia y eficiencia para los fines previstos, todas estas preocupaciones son vitales para cualquier tipo de organización.

TRANSFERIR EL RIESGO: El riesgo puede ser transferido de una organización a otra que tenga más capacidad de tratarlo.

UCLA: Universidad de California en Los Ángeles

USENET es el acrónimo de Users Network (Red de usuarios), consistente en un sistema global de discusión en Internet, que evoluciona de las redes UUCP. Fue creado por Tom Truscott y Jim Ellis, estudiantes de la Universidad de Duke, en 1979.