UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGON

"FUNDAMENTOS DE AUDITORIA INFORMATICA Y SU APLICACIÓN A LA SEGURIDAD EN REDES DE ORDENADORES"

T E S I S
QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACION

P R E S E N T A :
ERIKA VERONICA CHAVEZ CHAVEZ

ASESOR:
ING. DAVID MOISES TERAN PEREZ

MEXICO 2003

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

JEFATURA DE CARRERA DE INGENIERÍA EN COMPUTACIÓN

OFICIO:ENAR/JACO/0015/03.

ASUNTO: Asignacion de Jurado.

LIC. ALBERTO IBARRA ROSAS
SECRETARIO ACADÉMICO
P r e s e n t e .

Por este conducto me permito presentar a usted, nombre de los profesores que sugiero integren el Sinodo del Examen Profesional de la alumna **ERIKA VERÓNICA CHÁVEZ CHÁVEZ**, que presenta el tema de tesis **"FUNDAMENTOS DE AUDITORÍA INFORMÁTICA Y SU APLICACIÓN A LA SEGURIDAD EN REDES DE ORDENADORES"**

PRESIDENTE:	**MAT. LUIS FLORES RAMÍREZ**
VOCAL:	**ING. SILVIA VEGA MUYTOY**
SECRETARIO:	**ING. DAVID MOISÉS TERÁN PÉREZ**
SUPLENTE :	**ING. DONACIANO JIMÉNEZ VÁZQUEZ**
SUPLENTE:	**ING. GLADIS E. FUENTES CHÁVEZ**

Quiero subrayar que el director de tesis es el **Ing. David Moisés Terán Chávez**, el cual está incluido con base en lo que reza el reglamento de Exámenes Profesionales de ésta Escuela.

Sin otro en particular, me es grato enviarle un cordial saludo.

A T E N T A M E N T E
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, Edo. de México, enero 13 del 2003.
EL JEFE DE CARRERA

M. EN C. JESÚS DÍAZ BARRIGA ARCEO

c.c.p. Lic. Ma. Teresa Luna Sánchez.- Jefa del Departamento de Servicios Escolares.
Ing. David Moises Teran Pérez. Asesor.
Interesada.

JDA*vjd

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

SECRETARÍA ACADEMICA

M. en C. JESÚS DÍAZ BARRIGA ARCEO
Jefe de la Carrera de Ingeniería en Computación,
Presente.

En atención a la solicitud de fecha 13 de enero del año en curso, por la que se comunica que la alumna ERIKA VERONICA CHAVEZ CHAVEZ, de la carrera de Ingeniero en Computación, ha concluido su trabajo de investigación intitulado "FUNDAMENTOS DE AUDITORÍA INFORMÁTICA Y SU APLICACIÓN A LA SEGURIDAD EN REDES DE ORDENADORES", y como el mismo ha sido revisado y aprobado por usted, se autoriza su impresión; así como la iniciación de los trámites correspondientes para la celebración del Examen Profesional.

Sin otro particular, reitero a usted las seguridades de mi atenta consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 15 de enero del 2003
EL SECRETARIO

Lic. ALBERTO IBARRA ROSAS

C p Asesor de Tesis
C p Interesado.

AIR/vr

A MIS PADRES Y HERMANOS

Con la mayor gratitud por los esfuerzos realizados para que lograra terminar mi carrera profesional siendo para mi la mayor herencia .

A mi madre que es el ser mas maravilloso del mundo que me dio la vida, gracias por el apoyo moral, su cariño y comprensión.

A mi padre por que desde pequeña ha sido para mi un hombre grande y maravilloso que siempre he admirado.

Con amor, respeto y admiración.

ERIKA VERÓNICA CHAVEZ CHAVEZ

INTRODUCCIÓN.

En la actualidad, el costo de los equipos de cómputo ha disminuido considerablemente, mientras que sus capacidades y posibilidades de utilización han aumentado en forma inversa a la reducción de sus costos. Aunque los costos unitarios han disminuido (el de un Ordenador Personal), los costos totales de la computación (de equipos, sistemas, paquetes, recursos humanos, consumibles, etcétera) se han incrementado considerablemente.

Ello se debe a que, si bien la relación precio / memoria es menor, el tamaño de la memoria de los equipos y sus capacidades son mucho mayores, con procesadores y dispositivos que permiten acceso de más datos en mucho menos tiempo y que procesan la información en forma más rápida (memorias RAM y ROM), discos duros, etcétera).

Esto hace que, aunque se han reducido los costos, al aumentar sus capacidades y facilidades se ha incrementado el costo total, lo que ha tenido como consecuencia que los costos totales del uso no hayan disminuido en todos los casos. Las nuevas herramientas con que se cuenta (Internet, Extranet, comunicación, Bases de Datos, Multimedios, etcétera) hacen que también se pueda tener acceso a mayor información, aunque el costo total de los sistemas, así como la confiabilidad y seguridad con que se debe trabajar, sean muy altos.

En algunas ocasiones ha disminuido el costo de las aplicaciones, pero se tiene poca productividad en relación con la información y uso que se da a éstas. También se tiene poco control sobre la utilización de los equipos, existe un deficiente sistema de seguridad tanto física como lógica y se presenta una falta de confidencialidad de la información. Lo que se debe incrementar es la productividad, el control, la seguridad y la confidencialidad, para tener la información necesaria en el tiempo y en el lugar adecuados para poder tomar las mejores decisiones. Los siguientes puntos de la tecnología de información son particularmente notables:

- ✓ Una gran disponibilidad de Arquitectura de Sistemas *("Hardware")* de ordenadores muy poderosos y baratos, incluyendo la incorporación, a través de la miniaturización de poderosas capacidades, en diferentes dispositivos diseñados para usos personales y profesionales.
- ✓ Una gran disponibilidad de Paquetes y Programas *("Software")* poderoso, barato y relativamente accesible, con interfases de uso gráfico.
- ✓ A la medida de el Cliente, cambio de sistemas a paquetes y programas preempacados.

- ✓ Cambio de Ordenadores Principales *("Mainframe")* a Ordenadores de uso individual o aumentadas como parte de redes dedicadas a compartir información, así como Ordenadores Corporativas con los correspondientes cambios en la naturaleza, organización y localización de actividades de los sistemas de información, como el cambio a Ordenadores de usuario final.
- ✓ Incremento en la habilidad de los ordenadores para acceder datos en tiempo real o demorado, ambos en forma local o a través de acceso a facilidades remotas, incluyendo vía Internet.
- ✓ Captura de nuevos datos y el liderazgo en tecnología en almacenamiento máximo para incrementar la computarización, datos / información en textos, gráficas y video, con énfasis en la administración, presentación y comunicación de información, utilizando aproximaciones de multimedia.
- ✓ La cobertura de información y las tecnologías de comunicación afectan la forma en que se trabaja y se compra.
- ✓ Incremento del uso de Internet para unir individuos, intraorganizaciones, a través de sistemas tales como correo electrónico (E-mail), incluyendo world y wide web.
- ✓ El incremento en el uso de Internet para conducir comunicación entre organizaciones e individuos, a través de sistemas de comercio electrónico, tales como intercambio electrónico de datos (EDI) y sistema de transferencia electrónica de fondos (EFTS).
- ✓ Mercadeo masivo y distribución de productos de tecnología de información y servicios, tales como ordenadores, paquetes y programas preempacados, servicio de recuperación de datos en línea, correo electrónico y servicios financieros.
- ✓ Reducción de barreras de uso de sistemas, estimulando una gran penetración de sistemas de información dentro de organizaciones de todos los tamaños, de lucro o no lucrativas, para contadores y consejos de administración, y para propósitos estratégicos e incremento de papeles del usuario final de computadoras.
- ✓ Una amplia penetración de tecnología de información, tal como diseño de manufactura por medio de asistencia computarizada (CAD/CAM), sistemas de imágenes por computadora, sistemas de información para ejecutivos (EIS) y sistemas de reuniones en forma electrónica (EMS).
- ✓ Nuevas técnicas de desarrollo de sistemas, basados en tecnologías de información, tales como paquetes y programas de ingeniería de asistencia computarizada (CASE), programación orientada a objetos y tecnología de flujos (WORK-FLOW).
- ✓ Desarrollo continuo de soporte de sistemas inteligentes, incorporando sistemas expertos, redes neuronales, agentes inteligentes y otras ayudas de solución de problemas.
- ✓ Acceso a reingeniería de nuevos negocios, basado en la integración efectiva de tecnología de información y procesos de negocios.

Uno de los problemas más frecuentes en los centros de informática es la falta de una adecuada organización, que permita avanzar al ritmo de las exigencias de las organizaciones. A esto hay que agregar la situación que presentan los nuevos equipos en cuanto al uso de Bases de Datos, Redes y Sistemas de Información.

Lo anterior, combinado con la necesidad de una eficiente planeación estratégica y corporativa de las organizaciones y con una descentralización de equipos y centralización de la información, ha provocado que la complejidad de las decisiones y las dimensiones de los problemas en cuanto a la mejor forma de organizar el área de cómputo, requieran aplicar técnicas modernas de control y administración.

En muchos centros de informática también se desconoce el adecuado empleo de herramientas administrativas contables / financieras, tales como presupuestos, finanzas, costos, recursos humanos, organización, control, etcétera. Esto repercute en una inadecuada área de informática que no permite tomar decisiones con las características que deben tener las organizaciones actuales, lo cual hace que no se cuente con los controles para asegurar que esas decisiones no se desvíen de los objetivos.

La proliferación de la tecnología de información ha incrementado la demanda de control de los sistemas de información, como el control sobre la privacidad de la información y su integridad, y sobre los cambios de los sistemas.

Además, hay una preocupación sobre la caída de los sistemas y sobre la seguridad de la continuidad del procesamiento de la información, en caso de que los sistemas se "caigan". Otra área de preocupación es la proliferación de subsistemas incompatibles y el ineficiente uso de los recursos de sistemas.

Los sistemas tienen diferentes etapas, y una de ellas puede ser la utilización de las herramientas que nos proporcionan los mismos sistemas electrónicos. Para poder evaluar un Sistema de Información es necesario conocelo y controlarlo desde su inicio, siguiendo su proceso, que puede ser manual, mecánico, electrónico, o bien la combinación de éstos, hasta llegar a su almacenamiento, respaldos, seguridad y eficiencia en el uso de la información que proporcionan.

No basta, pues, conocer una parte o fase del sistema, como pueden ser los equipos de cómputo, que tan sólo vienen a ser una herramienta dentro de un sistema de información.

La Informática ha sido un área que ha cambiado drásticamente en los últimos años. En una generación, la tecnología ha cambiado tanto que lo que sorprendió hace algunos años: como la llegada de el Hombre a la Luna, o bien la creación del horno de microondas, hoy nos parece algo muy familiar.

En una década hemos visto el cambio en la Organización de la Informática: si hace poco era algo común la tarjeta perforada, hoy lo vemos como algo de un pasado muy remoto, y consideramos como algo normal el uso de microordenadores y de redes. Esto ha provocado que se tengan especialistas dentro del área de la Informática. Ya no podemos pensar en el personal de Informática que podía trabajar con microordenadores y con grandes computadoras, o bien en la persona que conocía en detalle sobre Bases de Datos y de Comunicaciones. Ahora se deben tener especialistas en cada una de las áreas. Una de éstas es la **Auditoría en Informática**, y en ella debemos de tener especialistas para cada una de las diferentes funciones que realizarán. Esto sin duda depende del tamaño del área de la Informática y de la Organización.

OBJETIVO GENERAL.

Establecer los Fundamentos de la Auditoria Informática y su Aplicación a la Seguridad en Redes de Ordenadores.

OBJETIVOS PARTICULARES.

1.- Establecer el Concepto de Auditoria así como, sus implicaciones en la Informática.

2.- Establecer los Fundamentos de la Planeación de la Auditoria Informática.

3.- Conocer la Evaluación de los Sistemas que Requiere la Auditoria Informática.

4.- Explicar la Auditoria de la Seguridad en Redes.

5.- Especificar la Interpretación de la Auditoria Informática en Redes de Ordenadores.

CAPÍTULO I.

CONCEPTO DE AUDITORÍA INFORMÁTICA.

I.1.- Auditoria.

Con frecuencia la palabra "Auditoria" se ha empleado incorrectamente y se le ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. Por eso se ha llegado a usar la frase *"tiene auditoria"*, como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoria. El concepto de auditoria es más amplio; no sólo detecta errores: es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la Organización, y lograr los objetivos propuestos, (Echenique, 2001).

La palabra auditoria viene del latín *auditorius*, y de ésta proviene "auditor", el que tiene la virtud de oír; el diccionario lo define como *"revisor de cuentas colegiado"*. (Nuevo Diccionario Español *Sopena*, 2002).

El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico, que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores en caso de que existan, o bien mejorar la forma de actuación.

Si se consulta nuevamente el diccionario se encuentra que eficacia es: *"virtud, actividad, fuerza para poder obrar"*, *mientras que eficiencia es "virtud y facultad para lograr un efecto determinado"*; es decir, es el poder lograr lo planeado con los menores recursos posibles, mientras que eficacia es lograr los objetivos. (Nuevo Diccionario Español *Sopena*, 2002).

El *Boletín C* de Normas de Auditoria del Instituto Mexicano de Contadores dice:

"La Auditoria no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo, son de carácter indudable. La auditoria requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben de seguirse y estimar los resultados obtenidos". (Instituto Mexicano de Contadores, 2001).

Así como existen Normas y Procedimientos específicos para la realización de auditorías contables, debe haber Normas y Procedimientos para la realización de auditorías en Informática como parte de una profesión. Éstas pueden estar basadas en las experiencias de otras profesiones, pero con algunas características propias y siempre guiándose por el concepto de que la auditoría debe ser más amplia que la simple detección de errores, y que además la auditoría debe evaluar para mejorar lo existente, corregir errores y proponer alternativas de solución.

I.2.- Informática.

El concepto de Informática es más amplio que el simple uso de equipos de cómputo o bien de procesos electrónicos. *"No existe una sola concepción acerca de qué es Informática; etimológicamente, la palabra Informática deriva del francés* informatique. *Este neologismo proviene de la conjunción de* information *(información) y* automatique *(automática). Su creación fue estimulada por la intención de dar una alternativa menos tecnocrática y menos mecanicista al concepto de proceso de datos".* (CIFCA, 1983).

En 1966, la Academia Francesa reconoció este nuevo concepto y lo definió del modo siguiente: *"Ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automáticas, de la información contemplada como vehículo del saber humano y de la comunicación en los ámbitos técnico, económico y social".*

Hacia principios de los años setenta, ya eran claras las limitaciones de esta definición, sobre todo por el hincapié en el uso de las máquinas. El principal esfuerzo por redefinir el concepto de Informática lo realizó en esa época la Oficina Intergubernamental de Informática (IBI) en aquel tiempo órgano asociado a la UNESCO. Este organismo, a través de los comités expertos convocados para ello, formuló en 1975 esta definición: *"Aplicación racional, sistemática de la información para el desarrollo económico, social y político".*

La IBI también dio en esa época una descripción del concepto Informática que, aunque no constituye una definición formal, resulta muy descriptiva: *"Ciencia de la política de la Información".*

En 1977, con la intención de actualizar y afinar el concepto, la Academia Mexicana de Informática propuso la siguiente definición: *"Ciencia de los sistemas inteligentes de información".*

En algunas ocasiones se ha empleado como sinónimos los conceptos de proceso electrónico, computadora e informática. El concepto de Informática es más amplio, ya que considera el total del sistema y el manejo de la información, la cual puede usar los equipos electrónicos como una de sus herramientas.

También es común confundir el concepto de dato con el de información. La información es una serie de datos clasificados y ordenados con un objetivo común. El dato se refiere únicamente a un símbolo, signo o una serie de letras o números, sin un objetivo que dé un significado a esa serie de símbolos, letras o números.

La información está orientada a reducir la incertidumbre del receptor y tiene la característica de poder duplicarse prácticamente sin costo, no se gasta. Además, no existe por sí misma, sino que debe expresarse en algún objeto (papel, cinta, disco, etcétera) de otra manera, puede desaparecer o deformarse, como sucede con la comunicación oral, lo cual hace que la información deba ser controlada debidamente por medio de adecuados sistemas de seguridad, confidencialidad y respaldo. (Álvarez, 1998).

La información puede comunicarse, y para ello hay que lograr que los medios de seguridad sean llevados a cabo después de un adecuado examen de la forma de transmisión, de la eficiencia de los canales de comunicación: el transmisor, el receptor, el contenido de la comunicación, la redundancia y el ruido.

La información ha sido dividida en varios niveles. El primero es el nivel técnico, que considera los aspectos de eficiencia y capacidad de los canales de transmisión; el segundo es el nivel semántico, que se ocupa de la información desde el punto de vista de su significado; el tercero es el pragmático, el cual considera al receptor en un contexto dado, y el cuarto nivel analiza la información desde el punto de vista normativo y de la parte ética, o sea considera cuándo, dónde y a quién se destina la información o la difusión que se le dé. La Informática debe abarcar los cuatro niveles de información. En el cuarto nivel se tiene una serie de aspectos importantes, como la parte legal del uso de la información, los estudios que se han hecho sobre la parte jurídica de la información y la creación de la ética informática, que no sólo debe incluir a los profesionales técnicos y especialistas en informática, sino también a los usuarios tanto de grandes ordenadores como de ordenadores personales. (Fernández, 2001).

La información tradicional (oral y escrita) se ve afectada dentro de la Informática cuando se introduce el manejo de medios electrónicos, lo cual la hace fácilmente modificable y adaptable a la características de cada receptor. La información también tiene la capacidad de manejarse en forma rápida y en grandes volúmenes, lo cual permite generar, localizar, duplicar y distribuir la información de modo sorprendente, a través de métodos, técnicas y herramientas como microordenadores, procesos distribuidos, redes de comunicación, Bases de Datos, etcétera.

La nueva tecnología permite que el usuario disponga de la información en cualquier momento, ya sea para su acceso, actualización, cambio o explotación o para que pueda distribuirse e intercambiarse entre tantos usuarios como se desee. Aunque al mismo tiempo se plantea un gran problema en cuanto al cuarto nivel de la información, que es su parte ética y el estudio de las posibilidades del buen o mal uso de la información por parte de personas no autorizadas.

La planeación y control de la información nos ofrece nuevos aspectos importantes a considerar, entre los que están la Teoría de Sistemas, las Bases de Datos, los Sistemas de Comunicación y los Sistemas de Información, que van a complementar el concepto de Informática y su campo de acción.

El Boletín E-02 del Instituto Mexicano de Contadores señala respecto al control interno: "El estudio y evaluación del control interno se efectúa con el objeto de cumplir con la Norma de Ejecución del Trabajo que requiere que: el auditor debe efectuar un estudio y evaluación adecuados del control interno existente, que le sirvan de base para determinar el grado de confianza que va a depositar en él, así mismo, que le permitan determinar la naturaleza, extensión y oportunidad que va a dar a los procedimientos de auditoría. El control interno comprende el Plan de Organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la razonabilidad y confiabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la Administración. (Instituto Mexicano de Contadores, 2002).

I. 2.1.- Objetivos Básicos del Control Interno.

De lo anterior se desprende que los cuatro objetivos básicos del control interno son:

- La protección de los activos de la Empresa.
- La obtención de información financiera veraz, confiable y oportuna.
- La promoción de la eficiencia en la operación del negocio.
- Lograr que en la ejecución de las operaciones se cumplan las políticas establecidas por los administradores de la Empresa.

Se ha establecido que los dos primeros objetivos abarcan el aspecto de controles internos contables y los dos últimos se refieren a controles internos administrativos. (Koontz, 2002).

I.2.2.- Objetivos Generales de Control Interno.

El control interno contable comprende el plan de organización y los procedimientos y registros que se refieren a la protección de los activos y a la confiabilidad de los registros financieros. Por lo tanto, está diseñado en función de los objetivos de la organización para ofrecer seguridad razonable de que las operaciones se realizan de acuerdo con las Normas y Políticas señaladas por la Administración, (Koontz, 2002). Cuando se habla de los objetivos de los controles contables internos se identifican dos niveles:

a). Objetivos generales de control interno aplicables a todos los sistemas.
b). Objetivos de control interno aplicables a ciclos de transacciones.

Los objetivos generales de control aplicables a todos los sistemas se desarrollan a partir de los objetivos básicos enumerados anteriormente, y son más específicos, para facilitar su aplicación. Los objetivos de control de ciclos se desarrollan a partir de los objetivos generales de control de sistemas, para que se apliquen a las diferentes clases de transacciones agrupadas en un ciclo, (Sánchez, 1997). Los objetivos generales de control interno de sistemas pueden resumirse a continuación:

1.- Los objetivos de autorización.- Todas las operaciones deben realizarse de acuerdo con autorizaciones generales o especificaciones de la Administración. Las autorizaciones deben estar de acuerdo con criterios establecidos por el nivel apropiado de la Administración. Las transacciones deben ser válidas para conocerse y ser sometidas oportunamente a su aceptación. Todas aquellas que reúnan los requisitos establecidos por la Administración deben reconocerse como tales y procesarse a tiempo. Los resultados del procesamiento de transacciones deben comunicarse oportunamente y estar respaldados por archivos adecuados.

2.- Objetivos del Procesamiento y Clasificación de Transacciones.- Todas las operaciones deben registrarse para permitir la preparación de Estados Financieros en conformidad con los principios de contabilidad generalmente aceptados, o con cualquier otro criterio aplicable a los estados y para mantener en archivos apropiados los datos relativos a los activos sujetos a custodia. Las transacciones deben clasificarse en forma tal que permitan la preparación de Estados Financieros en conformidad con los principios de contabilidad generalmente aceptados según el criterio de la Administración. Las transacciones deben quedar registradas en el mismo período contable cuidando de manera específica que se registren aquellas que afectan más de un ciclo.

3.- Objetivo de Salvaguarda Física.- El acceso a los activos sólo debe permitirse de acuerdo con autorizaciones de la Administración.

4.- Objetivo de Verificación y Evaluación.- Los datos registrados a los activos sujetos a custodia deben compararse con los activos existentes a intervalos razonables, y se deben tomar las medidas apropiadas respecto a las diferencias que existan. Así mismo, deben existir controles relativos a la verificación y evaluación periódica de los saldos que se incluyen en los Estados Financieros, ya que este objetivo complementa en forma importante los mencionados anteriormente.

Estos objetivos generales del control interno de sistemas son aplicables a todos los ciclos. No se trata de que se usen directamente para evaluar las técnicas de control interno de una Organización, pero representan una base para desarrollar objetivos específicos de control interno por ciclos de transacciones que sean aplicables a una Empresa individual.

El área de Informática puede interactuar de dos maneras en el control interno. La primera es servir de herramienta para llevar a cabo un adecuado control interno, y la segunda es tener un control interno del área y del departamento de Informática.

En el primer caso se lleva el control interno por medio de la evaluación de una Organización, utilizando el Ordenador como herramienta que auxiliará en el logro de los objetivos, lo cual se puede hacer por medio de paquetes de Auditoría. Esto debe ser considerado como parte del control interno con Informática. En el segundo caso se lleva a cabo el control interno de Informática. Es decir, como se señala en los objetivos del control interno, se deben proteger adecuadamente los activos de la Organización por medio del control, para que se obtenga la información en forma veraz, oportuna y confiable, para que se mejore la eficiencia de la operación de la Organización mediante la Informática, y para que en la ejecución de las operaciones de Informática se cumplan las políticas establecidas por la administración: todo ello debe ser considerado como control interno de Informática.

Al estudiar los objetivos del control interno se puede ver en primer lugar que, aunque en Auditoría en Informática el objetivo es más amplio, se deben tener en cuenta los objetivos generales del control interno aplicables a todo ciclo de transacciones. La Auditoría en Informática debe tener presentes los objetivos de autorización, procesamiento y clasificación de transacciones, así como los de salvaguarda física, verificación y evaluación de los equipos y de la información. La diferencia entre los objetivos de control interno desde un punto de vista contable financiero es que, mientras estos están enfocados a la evaluación de una Organización mediante la revisión contable financiera y de otras operaciones, los objetivos del control interno en Informática están orientados a todos los sistemas en general, al equipo de cómputo y al Departamento de Informática, para lo cual se requieren conocimientos de contabilidad, finanzas, recursos humanos, administración, etcétera, así como de experiencia y un saber profundo en Informática.

La auditoría interna debe estar presente en todas y cada una de las partes de la Organización. Ahora bien, la pregunta que normalmente se plantea es: ¿cuál debe ser su participación dentro del área de Informática?

La Informática es en primer lugar una herramienta muy valiosa que debe tener un adecuado control y es un auxiliar de la auditoría interna. Pero, según este concepto, la auditoría interna puede considerarse como un usuario del área de Informática. Se ha estudiado que los objetivos generales de control interno son:

- Autorización.
- Procesamiento y clasificación de las transacciones.
- Salvaguarda física.
- Verificación y evaluación.

Con base en los objetivos y responsabilidades del control interno se puede hacer otras dos preguntas: ¿de qué manera puede participar el personal de control interno en el sistema de los sistemas?, ¿qué conocimientos debe tener el personal de control interno para poder cumplir adecuadamente sus funciones dentro del área de Informática?

Las respuestas a estas preguntas dependerán del nivel que tenga el control interno dentro de la Organización. Sin embargo, en el diseño general y detallado de los sistemas se debe incluir a personal de la contraloría interna, que habrá de tener conocimientos de informática, aunque no se requerirá que sean especialistas, ya que sólo intervendrán en el diseño general del sistema, en el diseño de controles, en los sistemas de seguridad, en el respaldo y confidencialidad del sistema y en los sistemas de verificación. Se habrán de comprobar las fórmulas de obtención del impuesto sobre el producto del trabajo, el cálculo del pago del seguro social, etcétera; pero ya no deberán intervenir en la elaboración de los sistemas, Bases de Datos o programación. Tendrán que comprobar que los señalado en el diseño general sea igual a lo obtenido en el momento de implantación, para que puedan dar su autorización a la corrida en paralelo. El auditor interno, en el momento en que se están elaborando los sistemas, debe participar en estas etapas:

- Asegurarse de verificar que lo requerimientos de seguridad y de auditoría sean incorporados, y participar en la revisión de puntos de verificación.
- Revisar la aplicación de los sistemas y de control tanto con el usuario como en el Centro de Informática.
- Verificar que las políticas de seguridad y los procedimientos estén incorporados al plan en caso de desastre.
- Incorporar técnicas avanzadas de auditoría en los sistemas de cómputo.

Los sistemas de seguridad no pueden llevarse a cabo a menos que existan procedimientos de control y un adecuado plan en caso de desastre, elaborados desde el momento en el que se diseña el sistema.

El auditor interno desempeña una importante función al participar en los planes a largo plazo y en el diseño detallado de los sistemas y su implantación, detal manera que se asegure que los procedimientos de auditoría y de seguridad sean incorporados a todas y cada una de las fases del sistema.

I.3.- Auditoria Administrativa / Operacional.

La tecnología en información está afectando la forma en que las organizaciones están estructuradas, administradas y operadas. En algunos casos, los cambios son dramáticos. Cuando existe la necesidad de un nuevo diseño de sistemas administrativos para lograr una efectiva administración y control financiero, la planeación administrativa y el proceso de diseño y los requerimientos de control interno deberán cambiar o necesariamente se modificarán con los cambios de la tecnología de información. El incremento de la tecnología de información está soportado por una reestructuración organizacional alrededor de esta tecnología. La Auditoría Administrativa es: *"El examen global y constructivo de la estructura de una Empresa, de una Institución, una sección del gobierno o cualquier parte de un organismo, en cuanto a sus planes y objetivos, sus métodos y controles, su forma de operación y sus facilidades humanas y física"*. (Leonard, 2000).

Se lleva a cabo una revisión y consideración de la organización de una Empresa con el fin de precisar:

- Pérdidas y deficiencias.
- Mejores métodos.
- Mejores formas de control.
- Operaciones más eficientes.
- Mejor uso de los recursos físicos y humanos.

La Auditoría Administrativa debe llevarse a cabo como parte de la auditoría del área de Informática; se ha de considerar dentro del programa de trabajo de auditoría en informática, tomando principios de la Auditoría Administrativa para aplicarlos al área de Informática. El Departamento de Informática se deberá evaluar de acuerdo con:

- Objetivos, metas, planes, políticas y procedimientos.
- Organización.
- Estructura Orgánica.
- Funciones y niveles de autoridad y responsabilidad.

Además es importante tener en cuenta los siguientes factores:

- Elemento Humano.
- Organización (Manual de Organización).
- Integración.
- Dirección.
- Supervisión.
- Comunicación y Coordinación.
- Delegación.
- Recursos Materiales.
- Recursos Técnicos.
- Recursos Financieros.
- Control.

I.4.- Auditoria con Informática.

Los procedimientos de Auditoria con Informática varían de acuerdo con la filosofía y técnica de cada Organización y Departamento de Auditoria en particular. Sin embargo, existen ciertas técnicas y/o procedimientos que son compatibles en la mayoría de los ambientes de Informática. Estas técnicas caen en dos categorías: métodos manuales y métodos asistidos por ordenador.

En general, el auditor debe utilizar el ordenador en la ejecución de la auditoria, ya que esta herramienta permitirá ampliar la cobertura del examen, reduciendo el tiempo/costo de la pruebas y procedimientos de muestreo, que de otra manera tendrán que efectuarse manualmente. Existen paquetes de ordenadores que permiten elaborar auditorias a sistemas financieros y contables que se encuentran en medios informáticos. Además, el empleo del ordenador por el auditor le permite familiarizarse con la operación del equipo en el centro de cómputo de la Institución, (Porter y Thomas, 2001). Un Ordenador puede ser empleado por el auditor en:

- ✓ Transmisión de información de la contabilidad de la Organización al ordenador del auditor, para ser trabajada por éste, o bien acceso al sistema en red para que el auditor elabore las pruebas.
- ✓ Verificación de cifras totales y cálculos para comprobar la exactitud de los reportes de salida producidos por el Departamento de Informática, de la información enviada por medios de comunicación y de la información almacenada.
- ✓ Pruebas de los registros de los archivos para verificar la consistencia lógica, la validación de condiciones y la razonabilidad de los montos de las operaciones.
- ✓ Clasificación de datos y análisis de la ejecución de procedimientos.

- ✓ Selección e impresión de datos mediante técnicas de muestreo y confirmaciones.
- ✓ Llevar a cabo en forma independiente una simulación del proceso de transacciones para verificar la conexión y consistencia de los programas de ordenador.

Con fines de auditoria, el auditor interno puede emplear el ordenador para:

- ➢ Utilización de paquetes para auditoría; por ejemplo, paquetes provenientes del fabricante de equipos, firmas de contadores públicos o compañías desarrolladoras de paquetes y programas.
- ➢ Supervisar la elaboración de programas que permitan el desarrollo de la auditoria interna.
- ➢ Utilización de programas de auditoria desarrollados por proveedores de equipo, que básicamente verifican la eficiencia en el empleo del ordenador o miden la eficiencia de los programas, su operación o ambas cosas.

Todos los programas o paquetes empleados en la auditoría deben permanecer bajo estricto control del Departamento de Auditoria. Por esto, toda documentación, material de pruebas, listados fuente, programas fuente y objeto, además de los cambios que se les hagan, serán responsabilidad del auditor.

En aquellas instalaciones que cuentan con bibliotecas de programas catalogados, los programas de auditoría pueden ser guardados utilizando contraseñas de protección, situación que sería aceptable en tanto se tenga el control de las instrucciones necesarias para la recuperación y ejecución de los programas desde la biblioteca donde están almacenados. Los programas desarrollados con objeto de hacer auditoría deben estar cuidadosamente documentados para definir sus propósitos y objetivos y asegurar una ejecución continua. Cuando los programas de auditoría están siendo procesados, los auditores internos deberán asegurarse de la integridad del procesamiento mediante controles adecuados como:

- ❖ Mantener el control básico sobre los programas que se encuentren catalogados en el sistema y llevar a cabo protecciones apropiadas.
- ❖ Observar directamente el procesamiento de la aplicación de auditoría.
- ❖ Desarrollar programas independientes de control que verifiquen el procesamiento del programa de auditoria.
- ❖ Mantener el control sobre las especificaciones de los programas, documentación y comandos de control.
- ❖ Controlar la integridad de los archivos que se están procesando y las salidas generadas.

I.5.- Técnicas Avanzadas de Auditoría con Informática.

Cuando en una instalación se encuentren operando sistemas avanzados de computación, como procesamiento en línea, Bases de Datos y procesamiento distribuido, se podría evaluar el sistema empleando técnicas avanzadas de auditoría. Estos métodos requieren un experto y, por lo tanto, pueden no ser apropiados si el Departamento de Auditoría no cuenta con el entrenamiento adecuado. Otra limitante, incluyendo el costo, puede ser la sobrecarga del sistema y la degradación en el tiempo de respuesta. Sin embargo, cuando se usan apropiadamente, estos métodos supieran la utilización en una auditoría tradicional. (Piattini y del Peso, 1998).

1.- Pruebas Integrales.- Consisten en el procesamiento de datos de un departamento ficticio, comparando estos resultados con resultados predeterminados. En otras palabras, las transacciones iniciadas por el auditor son independientes de la aplicación normal, pero son procesadas al mismo tiempo. Se debe tener especial cuidado con las particiones que se están utilizando en el sistema para prueba de la contabilidad o balances, a fin de evitar situaciones anormales.

2.- Simulación.- Consiste en desarrollar programas de aplicación para determinada prueba y comparar los resultados de la simulación con la aplicación real.

3.- Revisiones de Acceso.- Se conserva un registro computarizado de todos los accesos a determinados archivos; por ejemplo, información de la identificación tanto de la terminal como del usuario.

4.- Operaciones en Paralelo.- Consiste en verificar la exactitud de la información sobre los resultados que produce un sistema nuevo que sustituye a uno ya auditado.

5.- Evaluación de un Sistema con Datos de Prueba.- Esta verificación consiste en probar los resultados producidos en la aplicación con datos de prueba contra los resultados que fueron obtenidos inicialmente en las pruebas del programa (solamente aplicable cuando se hacen modificaciones a un sistema).

6.- Registros Extendidos.- Consisten en agregar un campo de control a un registro determinado, como un campo especial a un registro extra, que pueda incluir datos de todos los programas de aplicación que forman parte del procesamiento de determinada transacción.

7.- Totales Aleatorios de Ciertos Programas.- Se consiguen totales en algunas partes del sistema para ir verificando su exactitud en forma parcial.

8.- Selección de Determinado Tipo de Transacciones como Auxiliar en el Análisis de un Archivo Histórico.- Por medio de este método se puede analizar en forma parcial el archivo histórico de un sistema, el cual sería casi imposible de verificar en forma total.

9.- Resultados de Ciertos Cálculos para Comparaciones Posteriores.- Con ellos se puede comparar en el futuro los totales en diferentes fechas.

Las técnicas anteriormente descritas ayudan al auditor interno a establecer una metodología para la revisión de los sistemas de aplicación de una Institución, empleando como herramienta el mismo equipo de cómputo. Sin embargo, actualmente se han desarrollado programas y sistemas de auditoría que eliminan los problemas de responsabilidad del Departamento de Auditoría, al intervenir en las actividades e información cuyo control corresponde estrictamente al Departamento de Informática, lo cual proporciona una verdadera independencia al auditor en la revisión de los datos del sistema. En la actualidad, el auditor puede estar desarrollando algunas de sus funciones al intervenir en las redes de comunicación interna. El empleo del microordenador en la auditoría constituye una herramienta que facilita la realización de actividades de revisión como:

- Trasladar los datos del sistema a u ambiente de control del auditor.
- Llevar a cabo la selección de datos.
- Verificar la exactitud de los cálculos: muestreo estadístico.
- Ordenamiento de la información. Producción de reportes e histogramas.

El auditor interno debe participar en el diseño general y específico de los sistemas, con el fin de asegurar que se tengan todos los controles de acuerdo con las políticas internas antes de que se comience la programación del sistema. A continuación se muestran ejemplos de las formas tradicionales de evidencia que existen en un proceso manual y las maneras en que el ordenador puede cambiarlas:

1.- Transacciones Originadas por Personas y Accedidas a un Sistema para su Proceso.- En las aplicaciones computarizadas, pueden generarse automáticamente. Por ejemplo, el sistema puede emitir automáticamente una orden de reposición cuando el inventario esté a un nivel por debajo del punto de reorden. Sin el ordenador se requeriría que una persona estuviera revisando y elaborara la orden de reposición cuando el inventario estuviera abajo del mínimo ya establecido.

2.- El Registro Manual de la Información necesaria para Originar una Transacción.- En las aplicaciones computarizadas no se producen documentos impresos cuando la información es accedida a un archivo maestro de nóminas computarizado a través de la red interna, sin dejar registro impreso del cambio, aunque se debe tener una clave de seguridad para poder accederlo y llevar un registro histórico en el que se tenga la información sobre la persona y terminal en la que se accedió la información.

3.- La Revisión de Transacciones por el Personal, que deja constancia con sus firmas, iniciales o sellos en los documentos para Indicar la Autorización del Proceso.- En las aplicaciones computarizadas la autorización puede ser automática. Por ejemplo, una venta a crédito puede ser automáticamente aprobada si el límite de crédito previamente determinado no está excedido. Otros métodos de autorización electrónica incluyen el acceso mediante claves de seguridad. Anteriormente, se tenían firmas en donde ahora sólo se tiene una clave o llave de acceso, que es equivalente a la autorización dejando únicamente un registro (en el mejor de los casos) de la llave de acceso utilizada, el lugar donde se tuvo acceso, la hora y el día en que fue autorizada.

4.- El Transporte de Documentos de una Estación de Trabajo a otra por Personas, Correo o Servicios Similares de un lugar del Negocio a otro sitio completamente Distinto.- Por estos medios se moviliza un documento físicamente. En aplicaciones computarizadas los datos pueden ser enviados electrónicamente. La información es transcrita, codificada, frecuentemente condensada y entonces enviada electrónicamente por líneas de comunicaciones, y al final queda un registro de cuándo recibió la información el receptor.

5.- Procesamiento Manual.- Generalmente, los documentos de las transacciones contienen espacio de trabajo para ejecutar el proceso necesario. En las aplicaciones computarizadas, el proceso se efectúa electrónicamente dentro de la memoria del ordenador mediante procedimientos programados y siguiendo reglas predeterminadas.

6.- Proceso Simplificado que facilita las Ejecuciones Repetitivas sin alta Probabilidad de Error.- En las aplicaciones computarizadas, el proceso puede ser extremadamente complejo debido a la velocidad y exactitud del ordenador. Por ejemplo, una Compañía puede utilizar su Ordenador para calcular la efectividad de cientos de posibles horarios o cédulas de producción a fin de seleccionar el más adecuado, mientras que en los métodos manuales esto sería casi imposible.

7.- Mantenimiento en Manuales de Información de naturaleza fija que es necesaria para el Proceso, como Tarifas de Nóminas o precios de Productos.- En las aplicaciones computarizadas, esta información se almacena en medios computarizados o bien por medio de catálogos, en los métodos manuales es difícil tener catálogos muy amplios y con actualización inmediata.

8.- Listado de los resultados del Proceso en documentos impresos, como cheques y reportes.- Frecuentemente, estos documentos contienen resultados de procesos intermedios. En las aplicaciones computarizadas el proceso puede no dar por resultados documentos impresos. Por ejemplo, los fondos pueden ser transferidos electrónicamente. En algunos sistemas, la información rutinaria es retenida de manera que sólo se recibe noticia de aquellas partidas que requieren acción.

9.- Almacenamiento de Documentos de Entrada, Proceso y Salida en Registro de Archivo o Similares.- Cuando la información es necesaria, puede localizarse y recobrarse manualmente del área de almacenamiento físico. En las aplicaciones computarizadas, la mayoría de los archivos están en medios magnéticos. Deben utilizarse programas extractivos para recobrar la información de tales medios, los cuales son normalmente muy rápidos y exactos; por ejemplo, en el caso de Bases de Datos.

10.- Uso de Documentos Impresos para Construir el Proceso.- En los procesos manuales estos documentos contienen información fuente, firmas de autorización, métodos de proceso y resultados de salida. Esta información usualmente es suficiente para construir la transacción y rastrearla hacia totales de control o, a partir de éstos, hasta el documento fuente. En las aplicaciones computarizadas las pistas de auditoría pueden verse fragmentadas, como frecuentemente ocurre en un ambiente de Base de Datos. Además, gran parte de la información que serviría de pista de auditoría puede estar almacenada en medios computarizados. Las pistas de auditoría computarizada a menudo requieren entender las reglas del proceso del sistema y no siempre es obvio cuáles pasos del proceso se ejecutaron, en especial cuando el proceso computacional es complejo.

11.- Uno o más Manuales de procedimientos que contienen Información relativa a las transacciones del Sistema.- Estos manuales guían a la gente en la circulación y proceso de las transacciones. En las aplicaciones computarizadas, pueden ser incluidos en los sistemas mediante ayudas.

12.- Revisión de Procesos por Personas, generalmente Supervisores, para determinar su razonabilidad, exactitud, totalidad y autorización.- En las aplicaciones computarizadas, gran parte de este monitoreo es ejecutado automáticamente mediante una lógica de programa predeterminada. Cada vez es más difícil para la gente monitorear los procesos, conforme los sistemas computacionales están más integrados y son más complejos y el ciclo del proceso se acorta; al mismo tiempo, el número de usuarios y responsables de la información es mayor.

13.- La División de Tareas entre los Empleados.- En las aplicaciones computarizadas, la distribución de deberes implica no sólo la división de tareas entre los empleados, sino también la división de tareas entre los pasos del proceso automatizado. Por ejemplo, los programas computarizados pueden procesar diferentes partes de una transacción en diversos lugares, y en ocasiones, se requiere que tengan sistemas de seguridad de acceso a nivel sistema, dato o programa, como en el caso de los sistemas bancarios.

14.- Proceso de grandes cantidades que puede requerir la repetición o cruzamiento de diversos elementos de la Información.- Esto es frecuentemente difícil y costoso en un sistema manual y sólo se realiza cuando es necesario.

En las aplicaciones computarizadas, grandes cantidades de datos pueden ser almacenados en una Base de Datos. La velocidad y capacidades de proceso del Ordenador hacen que esta información esté disponible en el formato deseado. En un ambiente computarizado, son posibles los más complejos análisis y los usos secundarios de los datos.

I.6.- Planeación de los Procedimientos de Auditoría con Informática.

El propósito principal de la planeación de las medidas de auditoría es incluir dentro de las aplicaciones las facilidades que permitan realizar las actividades de auditoría de la manera más fluida. La planeación de los servicios establece las facilidades tanto actuales como futuras que ofrece la Dirección de Informática. El auditor debe examinar este plan para establecer los requerimientos de auditoría necesarios. Para el funcionamiento de dichos procedimientos se requieren dentro de los programas rutinas que permitan acceder la información y sistemas independientes para la selección, sumarización, comparación y emisión de reportes.

El poder planear y realizar estas tareas implica un trabajo complicado pero que es necesario hacer. La computarización de las organizaciones ha dado por resultado una concentración de datos y funciones, que son seleccionados, correlacionados, resumidos y diseminados. En un ambiente computarizado típico, normalmente un dato puede actualizar muchos archivos. Es necesario que el auditor cuente con las herramientas adecuadas para poder seguir el rastro del mismo y también verificar que el sistemas esté realizando las funciones que supuestamente debe ejecutar; estas herramientas computarizadas le deben permitir detectar los errores y corregirlos posteriormente.

Es comprensible pensar que el auditor no es un programador especializado, por lo que es obligación de este grupo de proceso planear el desarrollo de estas herramientas de cómputo, atendiendo las solicitudes y recomendaciones de los auditores y aportando su propia experiencia. También debe participar en las pruebas en paralelo y en la implantación del sistema, para asegurarse de que todos los procedimientos, entradas y salidas son los solicitados por el usuario en el momento del diseño detallado, así como para evaluar que los cálculos realizados sean los correctos y, en general, para dar la aprobación del sistema una vez verificado que cumpla con los objetivos, flujo de información, controles y políticas del usuario y de la Organización, (Seen, 1998).

La participación del auditor interno en el diseño e implementación de un sistema es de suma importancia. Por ejemplo, la clasificación de la evidencia que se venía utilizando tradicionalmente, como la firma del funcionario para autorizar una transacción, se ve reemplazada por una clave de seguridad de acceso o la firma electrónica, aunque la introducción de un Ordenador no necesariamente cambia las formas de la evidencia de auditoría.

El auditor debe estar presente en el desarrollo del sistema para evaluar que la información requerida por el usuario quede cubierta y se cumpla con el grado de control que necesita la información procesada por el sistema, de acuerdo con los objetivos y políticas de la Organización. Existen ciertas habilidades fundamentales que deben ser consideradas como las mínimas que todo auditor de Informática debe tener:

- Habilidad para manejar paquetes de procesadores de texto.
- Habilidades para manejo de hojas de cálculo.
- Habilidad para el uso de correo electrónico y conocimiento(s) de Internet.
- Habilidad para manejo de Bases de Datos.
- Habilidad para el uso de al menos un paquete básico de contabilidad.

Como evaluador, el auditor de Informática debe ser capaz de distinguir entre los procesos de evaluación de sistemas y las aproximaciones que son apropiadas para encauzar los propósitos específicos de evaluación relevante para el área de trabajo. En este sentido, el auditor en Informática debe tener los conocimientos de los pasos requeridos para aplicar una evaluación particular en el contexto de la tecnología de la información.

Debe poseer estándares (normas) relevantes y prácticas que gobiernen la conducción de una evaluación particular. Su contribución potencial a una evaluación particular puede ser hecha en un contexto específico. Las habilidades técnicas requeridas por el auditor en Informática son las de implantar, ejecutar y comunicar los resultados de la evaluación en el contexto de la tecnología de información, de acuerdo con estándares profesionales que gobiernen el objetivo de la auditoría.

I.7.- Concepto de Auditoría Informática.

Después de analizar los conceptos de Auditoría y de Informática, los diferentes tipos de auditoría, así como su interrelación con laInformática, se debe responder las siguientes preguntas: ¿qué es Auditoría Informática?, ¿cuál es su campo de acción? Algunas de las posibles respuestas so las siguientes, de acuerdo a diferentes autores:

"Es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de ordenadores, mantener la integridad de los datos y lograr los objetivos de la Organización en forma eficaz y eficiente". (Hernández, 1996).

"Auditoria Informática es la verificación de los controles en las siguientes tres áreas de la organización (informática)", Porter, (2002):

- *Aplicaciones (programas de producción).*
- *Desarrollo de Sistemas.*
- *Instalación del Centro de Proceso.*

Por tanto, se puede decir que Auditoría Informática es la revisión y evaluación de los controles, sistemas y procedimientos de la Informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la Organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones.

La información contenida depende de la habilidad de reducir la incertidumbre alrededor de las decisiones. El valor de la reducción de la incertidumbre depende del pago asociado con la decisión que se realiza. Los factores que pueden influir en una Organización a través del control y la Auditoría en Informática son:

- ✓ Necesidad de controlar el uso evolucionado de los ordenadores.
- ✓ Controlar el uso del ordenador, que cada día se vuelve más importante y costoso.
- ✓ Los altos costos que producen los errores en una Organización.
- ✓ Abuso en los ordenadores.
- ✓ Posibilidad de pérdida de capacidades de procesamiento de datos.
- ✓ Posibilidad de decisiones incorrectas.
- ✓ Valor de los sistemas (arquitectura, paquetes y programas) y del personal que los utiliza.
- ✓ Necesidad de mantener la privacidad individual.
- ✓ Posibilidad de pérdida de información o mal uso de ésta.
- ✓ Toma de decisiones incorrectas.
- ✓ Necesidad de mantener la privacidad de la Organización.

La información es un recurso necesario para la Organización y para la continuidad de las operaciones, ya que provee de una imagen de su ambiente actual, su pasado y su futuro. Si la imagen de la Organización es apropiada, ésta crecerá adaptándose a los cambios de su entorno. (Instituto Mexicano de Contadores Públicos, 2000).

En el proceso de la información se deben detectar sus errores u omisiones, y evitar su destrucción por causas naturales (temblores, inundaciones, incendios, etcétera) o cualquier contingencia que pudiera suscitarse. La toma de decisiones incorrectas, producto de datos erróneos proporcionados por los sistemas, trae como consecuencia efectos significativos que afectan directamente a la Organización.

El mayor estímulo para el desarrollo de la auditoría en Informática dentro de la Organización normalmente está dado por el abuso en el uso de los ordenadores. El abuso en ordenadores es cualquier incidente asociado con la tecnología en computación, en el cual la víctima sufra o pueda sufrir una pérdida y un daño hechos intencionalmente o para obtener una ganancia.

El problema más serio está en los errores u omisiones que causan pérdidas a la Organización. En seguida está el desastre de los ordenadores debido a causas naturales, tales como fuego, agua o fallas en el suministro eléctrico. Las técnicas de control que manejan estos dos tipos de problemas han sido mejor desarrolladas que aquellas que se relacionan con el abuso de los ordenadores.

El control en el abuso de los ordenadores es normalmente más difícil debido a lo inadecuado de las leyes. Es más difícil condenar a alguien que hizo un inadecuado uso del tiempo de los ordenadores, o copias ilegales de programas, debido a que las leyes no consideran a las computadoras como una persona, y sólo las personas pueden ser declaradas como culpables, o bien considerar a la información como un bien tangible y un determinado costo.

El abuso tiene una importante influencia en el desarrollo de la auditoría en Informática, ya que en la mayoría de las ocasiones el propio personal de la Organización es el principal factor que puede provocar las pérdidas dentro del área de Informática. Los abusos más frecuentes por parte del personal son la utilización del equipo en trabajo distintos a los de la Organización, la obtención de información para fines personales (Internet), los juegos o pasatiempos y los robos hormiga, además de los delitos informáticos que en muchas ocasiones también son llevados a cabo por el propio personal de la Organización. (Weber, 2001).

La Auditoría en Informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, comunicación, controles, archivos, seguridad, personal (desarrollador, operador, usuarios) y obtención de información. En esto se deben incluir los equipos de cómputo, por se la herramienta que permite obtener una información adecuada y una organización específica (departamento de cómputo, departamento de informática, gerencia de procesos electrónicos, etcétera), y el personal de hará posible el uso de los equipos de cómputo.

Además de los datos, la arquitectura de sistemas, los paquetes y programas y el personal, son recursos críticos de las organizaciones. Algunas de éstas tienen inversiones en equipo de cómputo con un valor multimillonario. Aun con un seguro adecuado, las pérdidas intencionales o no intencionales pueden causar daños considerables. En forma similar, los paquetes y programas muchas veces constituye una inversión muy importante.

Si los paquetes y programas son corrompidos o destruidos, es posible que la Organización no pueda continuar con sus operaciones, si no es prontamente recobrado. Si los paquetes y programas son robados, se puede proporcionar información altamente confidencial a la competencia, y si los paquetes y programas son de su propiedad, pueden tenerse pérdidas en ganancias o bien en juicios legales. Finalmente, el personal es siempre un recursos valioso, sobre todo ante la falta de personal de informática bien entrenado.

Los ordenadores ejecutan automáticamente muchas funciones críticas en la Sociedad. Consecuentemente, las pérdidas pueden ser muy altas y pueden ir desde pérdidas multimillonarias en lo económico, hasta pérdidas de libertad o de la vida en el caso de errores en laboratorios médicos o en hospitales.

Además de los aspectos constitucionales y legales, muchos países han considerado la privacidad como parte de los derechos humanos. Consideran que es responsabilidad de las personas que están en los ordenadores y con las redes de comunicación, asegurar que el uso de la información sea recolectada, integrada y entregada rápidamente y con la privacidad y confidencialidad requeridas. Existe una responsabilidad adicional en el sentido de asegurarse de que la información sea usada solamente para los propósitos que fue elaborada. (Rangel, 1998).

En este caso se encuentran las Bases de Datos, las cuales pueden ser usadas para fines ajenos para los que fueron diseñadas o bien entrar en la privacidad de las personas.

La tecnología es neutral, no es buena ni es mala. El uso de la tecnología es lo que puede producir problemas sociales. Por ejemplo, el mal uso de la tecnología en Internet no es problema de la tecnología, sino de la forma y características sobre las cuales se usa esa tecnología.

Es una función del gobierno, de las asociaciones profesionales y de los grupos de presión evaluar el uso de la tecnología; pero es bien aceptado el que las organizaciones en lo individual tengan una conciencia social, que incluya el uso de la tecnología en informática.

Deberá de existir una Legislación más estricta en el uso de la tecnología, en la que se considere el análisis y la investigación para evitar el mal uso de Internet y otras tecnologías, para evitar situaciones como el suicidio colectivo de sectas religiosas como sucedió en los Estados Unidos de América.

También se requiere de una ética por parte de las organizaciones y de los individuos que tienen en sus manos todo tipo de tecnología, no sólo la de informática.

I.8.- Campo de la Auditoria en Informática.

El campo de acción de la Auditoria Informática es según Willmar, (2001):

- La evaluación administrativa del área de Informática.
- La evaluación de los sistemas y procedimientos, y de la eficiencia que se tiene en el uso de la información. La evaluación de la eficiencia y eficacia con la que se trabaja.
- La evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (paquetes y programas, arquitectura de sistemas, bases de datos, comunicaciones, etcétera).
- Seguridad y confidencialidad de la información.
- Aspectos legales de los sistemas y de la información.

Para lograr los puntos anteriores se necesita:

a). Evaluación administrativa del Departamento de Informática. Esto comprende la evaluación de:

- Los objetivos del departamento, dirección o gerencia.
- Metas, planes, políticas y procedimientos de procesos electrónicos estándares.
- Organización del área y su estructura orgánica.
- Funciones y niveles de autoridad y responsabilidad del área de procesos electrónicos.
- Integración de los recursos materiales y técnicos.
- Dirección.
- Costos y controles presupuestales.
- Controles administrativos del área de procesos electrónicos.

b). Evaluación de los sistemas y procedimientos, y de la eficiencia y eficacia que se tienen en el uso de la información, lo cual comprende:

- Evaluación del análisis de los sistemas y sus diferentes etapas.
- Evaluación del diseño lógico del sistema.
- Evaluación del desarrollo físico del sistema.
- Facilidades para la elaboración de los sistemas.
- Control de proyectos.

- Control de sistemas y programación.
- Instructivos y documentación.
- Formas de implantación.
- Seguridad física y lógica de los sistemas.
- Confidencialidad de los sistemas.
- Controles de mantenimiento y forma de respaldo de los sistemas.
- Utilización de los sistemas.
- Prevención de factores que puedan causar contingencias; seguros y recuperación en caso de desastre.
- Productividad.
- Derechos de autor y secretos industriales.

c). Evaluación del proceso de datos y de los equipos de cómputo que comprende:

- Controles de los datos fuente y manejo de cifras de control.
- Control de operación.
- Control de salida.
- Control de asignación de trabajo.
- Control de medios de almacenamiento masivos.
- Control de otros elementos de cómputo.
- Control de medios de comunicación.
- Orden en el centro de cómputo.

D). Seguridad:

- Seguridad física y lógica.
- Confidencialidad.
- Respaldos.
- Seguridad personal.
- Seguros.
- Seguridad en la utilización de los equipos.
- Plan de contingencia y procedimiento de respaldo para casos de desastre.
- Restauración de equipos y de sistemas.

Los principales objetivos de la Auditoría Informática son:

- Salvaguardar los activos. Se refiere a la protección de la arquitectura de sistemas (equipos), paquetes y programas así como, de los recursos humanos.
- Integridad de datos. Los datos deben mantener consistencia y no duplicarse.
- Efectividad de sistemas. Los sistemas deben cumplir con los objetivos de la Organización.
- Eficiencia de sistemas. Que se cumplan los objetivos con los menores recursos.
- Seguridad y confidencialidad.

Para que sea eficiente la Auditoría en Informática, ésta se debe realizar también durante el proceso de diseño del sistema. Los diseñadores de sistemas tienen la difícil tarea de asegurarse que interpretan las necesidades de los usuarios, que diseñan los controles requeridos por los auditores y que aceptan y entienden los diseños propuestos.

La interrelación que debe existir entre la Auditoría en Informática y los diferentes tipos de auditoría es la siguiente: el núcleo o centro de la Informática son los programas, los cuales pueden ser auditados por medio de la auditoría de programas. Estos programas se usan en los ordenadores de acuerdo con la organización del centro de cómputo (personal).

La Auditoría en Informática debe evaluar todo (informática, organización del centro de cómputo, ordenadores, comunicaciones y programas), con auxilio de los principios de auditoría administrativa, auditoría interna, auditoría contable/financiera y, a su vez, puede proporcionar información a esos tipos de auditoría. Los ordenadores deben ser una herramienta para la realización de cualquiera de las auditorías.

La adecuada salvaguarda de los activos, la integridad de los datos y la eficiencia de los sistemas solamente se pueden lograr si la administración de la organización desarrolla un adecuado sistema de control interno.

El tipo y características del control interno dependerán de una serie de factores; por ejemplo, si se trata de un medio ambiente de miniordenadores o macroordenadores, si están conectados en serie o trabajan en forma individual, si se tiene Internet y Extranet. Sin embargo, la división de responsabilidades y la delegación de autoridad es cada vez más difícil debido a que muchos usuarios comparten recursos, lo que dificulta el proceso de control interno.

Como se ve, la evaluación que se debe desarrollar para la realización de la Auditoría en Informática debe ser hecha por personas con un alto grado de conocimiento en Informática y con mucha experiencia en el área. La información proporcionada debe ser confiable, oportuna, verídica, y debe manejarse en forma segura y con la suficiente confidencialidad, pero debe estar contenida dentro de parámetros legales y éticos.

I.9.- Auditoría de Programas.

La Auditoría de Programas es la evaluación de la eficiencia técnica, del uso de diversos recursos (cantidad de memoria) y del tiempo que utilizan los programas, su seguridad y confiabilidad, con el objetivo de optimizarlas y evaluar el riesgo que tienen para la Organización, (Fundación Arturo Rosemblueth, 2000).

La Auditoría de Programas tiene un mayor grado de profundidad y de detalle que la Auditoría en Informática, ya que analiza y evalúa la parte central del uso de los ordenadores, que es el programa, aunque se puede considerar como parte de la Auditoría en Informática.

Para lograr que la Auditoría de Programas sea eficiente, las personas que las realicen han de poseer conocimientos profundos sobre sistemas operativos, sistemas de administración de bases de datos, medios de comunicación y acerca del equipo en que fue escrito el programa. Así mismo, se deberá comenzar con la revisión de la documentación del mismo.

Para poder llevar a cabo la auditoría adecuada de los programas se necesita que los sistemas estén trabajando correctamente, y que se obtengan los resultados requeridos, ya que al cambiar el proceso del sistema en general se cambiarán posiblemente los programas. Sería absurdo intentar optimizar un programa de un sistema que estuviera funcionando correctamente. Para optimizar los programas se deberá tener pleno conocimiento y aceptación del sistema o sistemas que usan ese programa, y disponer de toda la documentación detallada del sistema total.

CAPÍTULO II.

PLANEACIÓN DE LA AUDITORÍA INFORMÁTICA.

II.1.- Fases de la Auditoria.

La Auditoría en Informática es el proceso de recolección y evaluación de evidencias para determinar cuándo son salvaguardados los activos de los sistemas computarizados, de qué manera se mantiene la integridad de los datos y cómo de logran los objetivos de la Organización eficazmente y se usan los recursos consumidos eficientemente. La Auditoría en Informática sigue los objetivos tradicionales de la auditoría: aquellos que son de la auditoría externa, de salvaguarda de los activos y la integridad de datos, y los objetivos gerenciales, aquellos propios de la auditoría interna que no sólo logran los objetivos señalados sino también los de eficiencia y eficacia, (Knudson y Woodworth, 2002).

La auditoria interna es una función independiente de la evaluación que se establece dentro de una Organización para examinar y evaluar sus actividades. El objetivo de la auditoría interna consiste en apoyar a los miembros de la Organización en el desempeño de sus responsabilidades. Para ello, proporciona análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas.

Los auditores internos son responsables de proporcionar información acerca de la adecuación y efectividad del sistema de control interno de la organización y de la calidad de la gestión.

El Manual de Organización deberá establecer claramente los propósitos del Departamento de Auditoría Interna, especificar que el alcance del trabajo no deberá tener restricciones y señalar que los auditores internos no tendrán autoridad y/o responsabilidad respecto de las actividades que auditan. El auditor interno debe ser independiente de las actividades que audita. Esta independencia permite que el auditor interno realice su trabajo libre y objetivamente, ya que sin esta independencia no se puede obtener los resultados deseados. Las Normas de Auditoría Interna comprenden:

- Las actividades auditadas y la objetividad de los auditores internos.
- El conocimiento técnico, la capacidad y el cuidado profesional de los auditores internos con los que deben ejercer su función. En el caso de la Auditoría en Informática es de suma importancia el que el auditor cuente con los conocimientos técnicos actualizados y con la experiencia necesaria en el área.
- El alcance del trabajo de auditoría interna en el área de Informática.
- El desarrollo de las responsabilidades asignadas a los auditores internos responsables de la Auditoría a Informática.

Los auditores internos deben ser independientes de las actividades que auditan, y deben de tener un amplio criterio para no tomar decisiones subjetivas basadas en preferencias personales sobre determinado equipo o programa(s), sin analizar a profundidad las opiniones. Los auditores internos son independientes cuando pueden desempeñar su trabajo con libertad y objetividad. La independencia permite a los auditores internos rendir juicios imparciales, esenciales para la adecuada conducción de las auditorías, esto se logra a través de una adecuada objetividad y criterio.

La objetividad es una actitud de independencia mental que los auditores internos deben mantener al realizar las auditorías. Los auditores internos no deben subordinar sus juicios en materia de auditoría al de otros. La objetividad requiere que los auditores internos realicen sus auditorías de tal manera que tengan una honesta confianza en el producto de su trabajo y que no hayan creado compromisos significativos en cuanto a la calidad. Los auditores internos no deben colocarse en situaciones en las que se sientan imposibilitados para hacer juicios profesionales objetivos.

Los resultados del trabajo de auditoría deben ser revisados antes de emitir el respectivo informe de auditoría, para proporcionar una razonable seguridad de que el trabajo se realizó objetivamente. El auditor en informática debe contar con los conocimientos técnicos requeridos y con capacidad profesional.

El Departamento de Auditoría Interna deberá asignar a cada auditoría a aquellas personas que en su conjunto posean los conocimientos, la experiencia y la disciplina necesarios para conducir apropiadamente la auditoría. También deberá asegurarse que la experiencia técnica y la formación académica de los auditores sean las apropiadas para realizar las auditorías en Informática, (Schulthers y Sumner, 1998).

El Departamento de Auditoría Interna deberá contar u obtener los conocimientos, experiencias y disciplinas necesarias para llevar a cabo sus responsabilidades de Auditoría en Informática. Deberá tener personal o emplear colsultores calificados en las disciplinas de informática necesarias para cumplir con las responsabilidades de auditoría; sin embargo, cada miembro del departamento no necesita estar calificado en todas las disciplinas. El Departamento de Auditoría Interna deberá asegurarse de:

- ✓ Que las auditorías sean supervisadas en forma apropiada. La supervisión es un proceso continuo que comienza con la planeación y termina con el trabajo de auditoría.
- ✓ Que los informes de auditoría sean precisos, objetivos, claros, concisos, constructivos y oportunos.
- ✓ Que se cumplan los objetivos de la auditoría.
- ✓ Que la auditoría sea debidamente documentada y que se conserve la evidencia apropiada de la supervisión.
- ✓ Que los auditores cumplan con las Normas profesionales de conducta.
- ✓ Que los auditores en Informática posean los conocimientos, experiencias y disciplinas esenciales para realizar sus auditorías.

Cada auditor interno requiere de ciertos conocimientos y experiencias:

- Se requiere pericia en la aplicación de las Normas, procedimientos y técnicas de auditoría interna para el desarrollo de las revisiones. Se entiende por pericia la habilidad para aplicar los conocimientos que se poseen a las situaciones que posiblemente se encuentren, ocupándose de ellas sin tener que recurrir en exceso a ayudas o investigaciones técnicas.
- Tener habilidad para: aplicar amplios conocimientos a situaciones que posiblemente se vayan encontrando, reconocer las desviaciones significativas y poder llevar a cabo las investigaciones necesarias para alcanzar soluciones razonables.

Entre las habilidades que deben tener los auditores están:

- Habilidad para comunicarse efectivamente y dar un trato adecuado a las personas. Los auditores internos deben tener habilidades para comunicarse tanto de manera oral como escrita, de tal manera que puedan transmitir clara y efectivamente asuntos como: los objetivos de la auditoría, las evaluaciones, las conclusiones y las recomendaciones.
- Los auditores en Informática son responsables de continuar su desarrollo profesional para poder mantener su pericia profesional. Deberán mantenerse informados acerca de las mejoras y desarrollos recientes.
- Los auditores en Informática deben ejercer el debido cuidado profesional al realizar sus auditorías. EL cuidado profesional, deberá estar de acuerdo con la complejidad de la auditoría que se realiza. Los auditores deben estar atentos a la posibilidad de errores intencionales, de errores, omisiones, de la ineficiencia, del desperdicio, de la inefectividad y del conflicto de intereses. También deberán estar alertas ante aquellas condiciones y actividades donde es más probable que existan irregularidades. Además, deberán de identificar los controles inadecuados y emitir recomendaciones para promover el cumplimiento con procedimientos y prácticas aceptables.

El debido cuidado implica una razonable capacidad, no infabilidad ni acciones extraordinarias. Requiere que el auditor realice exámenes y verificaciones con un alcance razonable, pero no requiere auditorías detalladas de todas las operaciones. Por consiguiente, el auditor no puede dar una absoluta seguridad de que no existan incumplimientos e irregularidades. Sin embargo, la posibilidad de que existan irregularidades materiales o que no se cumplan las disposiciones debe ser considerada siempre que el auditor emprende una auditoría, (Trickner, 1996).

Cuando el auditor detecte una irregularidad que va en contra de lo establecido deberá informarlo a las autoridades adecuadas de la Organización. El auditor puede recomendar cualquier investigación que considere necesaria en esas circunstancias. Posteriormente, el auditor deberá efectuar su seguimiento para verificar que se ha cumplido con lo señalado. El ejercicio del debido cuidado profesional significa el uso razonable de las experiencias y juicios en el desarrollo de la auditoría. Para este fin el auditor deberá considerar:

- El alcance del trabajo de auditoría necesario para lograr los objetivos de la auditoría.
- La materialidad o importancia de los asuntos a los que se aplican los procedimientos de la auditoría.
- La adecuación y efectividad de los controles internos.
- El costo de la auditoría en relación con los posibles beneficios.

El cuidado profesional incluye la evaluación de los estándares establecidos, determinando en consecuencia si tales estándares son aceptables y si son cumplidos. Cuando éstos son vagos deberán solicitarse interpretaciones autorizadas.

El alcance de la auditoría debe abarcar el examen y evaluación de la adecuación y efectividad del Sistema de Control Interno de la Organización y la Calidad en el cumplimiento de las responsabilidades asignadas. El propósito de revisar la adecuación del Sistema de Control Interno es cerciorarse si el sistema establecido proporciona una razonable seguridad de que los objetivos y metas de la Organización se cumplirán eficiente y económicamente. Los objetivos elementales del control interno son para asegurar:

- La confiabilidad e integridad de la información. Los auditores deben revisar la confiabilidad e integridad de la información y los métodos empleados para identificar, medir, clasificar y reportar dicha información.
- El cumplimiento de las políticas, planes, procedimientos, leyes y reglamentos.
- La salvaguarda de los activos.
- El uso eficiente y económico de los recursos.
- El logro de los objetivos y metas establecidos para las operaciones o programas.

El sistema de información proporciona datos para la toma de decisiones, el control y el cumplimiento con requerimientos externos. Por ello, los auditores deben examinar los sistemas de información y cuando sea apropiado asegurarse:

- Que los registros e informes contengan información precisa, confiable, oportuna, completa y útil.
- Que los controles sobre los registros e informes sean adecuados y efectivos.

Los auditores deben revisar los sistemas para asegurarse del cumplimiento de las políticas, planes y procedimientos, leyes y reglamentos que pueden tener un impacto significativo en las operaciones e informes, y deben determinar si la organización cumple con ellos.

La Gerencia de Informática es responsable del establecimiento de los sistemas diseñados para asegurar el cumplimiento de requerimientos tales como políticas, planes, procedimientos y leyes y reglamentos aplicables. Los auditores son responsables de determinar si los sistemas son adecuados y efectivos y si las actividades auditadas están cumpliendo con los requerimientos apropiados. Los auditores deberán revisar:

- La corrección de los métodos de salvaguarda de los activos y verificar la existencia de estos activos.
- Los métodos empleados para salvaguardar los activos de diferentes tipos de riesgos tales como: robo, incendio, actividades impropias o ilegales, así como de elementos naturales como terremotos, inundaciones, ciclones, etcétera.

Los auditores deberán evaluar si el empleo de los recursos se realiza en forma económica y eficiente. La administración es responsable de establecer estándares de operación para medir la eficiencia y economía en el uso de los recursos. Los auditores internos son responsables de determinar si:

Los estándares para medir la economía y eficiencia en el uso de los recursos son los adecuados.

Los estándares de operación establecidos han sido entendidos y se cumplen.

Las desviaciones a los estándares de operación se identifican, analizan y se comunican a los responsables para que tomen las medidas correctivas.

Se toman las medidas correctivas.

Las auditorías relacionadas con el uso económico y eficiente de los recursos deberán identificar situaciones tales como:

- Subutilización de instalaciones.
- Trabajo no productivo.
- Procedimientos que no justifican su costo.

- Exceso o insuficiencia de personal.
- Uso indebido de las instalaciones.

Los auditores deberán revisar las operaciones o programas para cerciorarse si los resultados son consistentes con los objetivos y metas establecidos y si las operaciones o programas se llevan a cabo como planearon.

II.2.- Planeación de la Auditoría en Informática.

Para hacer una adecuada planeación de la Auditoría en Informática hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismos a auditar, sus sistemas, organización y equipo. Con ello se puede determinar el número y características del área dentro del organismo a auditar, sus sistemas, organización y equipo. Con ello se puede determinar el número y características del personal de auditoría, las herramientas necesarias, el tiempo y costo, así como definir los alcances de la auditoría para, en caso necesario, poder elaborar el contrato de servicios, (Haag, 2000).

Dentro de la auditoría en general, la planeación es uno de los pasos más importantes, ya que una inadecuada planeación provocará una serie de problemas que pueden impedir que se cumpla con la auditoría o bien hacer que no se efectúe con el profesionalismo que debe tener cualquier auditor. El trabajo de auditoría deberá incluir la planeación de la auditoría, el examen y la evaluación de la información, la comunicación de los resultados y el seguimiento. La planeación deberá ser documentada e incluirá:

- ✓ El establecimiento de los objetivos y el alcance del trabajo.
- ✓ La obtención de información de apoyo sobre las actividades que se auditarán.
- ✓ La determinación de los recursos necesarios para realizar la auditoría.
- ✓ El establecimiento de la comunicación necesaria con todos los que estarán involucrados en la auditoría.
- ✓ La realización, en la forma más apropiada, de una inspección física para familiarizarse con las actividades y controles a auditar, así como la identificación de las áreas en las que se deberá hacer énfasis al realizar la auditoría y promover comentarios y la promoción de los auditados.
- ✓ La preparación por escrito del programa de auditoría.
- ✓ La determinación de cómo, cuándo y a quién se le comunicarán los resultados de la auditoría.
- ✓ La obtención de la aprobación del plan de trabajo de la auditoría.

En el caso de la Auditoría en Informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de varios objetivos:

- Evaluación administrativa del área de procesos electrónicos.
- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.
- Evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (paquetes y programas, la arquitectura de sistemas, redes, Bases de Datos, comunicaciones).
- Seguridad y confidencialidad de la información.
- Aspectos legales de los sistemas y de la información.

Para lograr una adecuada planeación, lo primero que se requiere es obtener información general sobre la Organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, y con base en esto planear el programa de trabajo, el cual deberá incluir tiempos, costos, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la auditoría. EL proceso de planeación comprende el establecer:

- Metas.
- Programas.
- Planes y contratación de personal y presupuesto financiero.
- Informes de actividades.

Las metas se deberán establecer de tal manera que se pueda lograr su cumplimiento, sobre la base de los planes específicos de operación y de los presupuestos, los que hasta donde sea posible deberán ser cuantificables. Deberán acompañarse de los criterios para mediarlas y de fechas límite para su logro.

Los programas de trabajo de auditoría deberán incluir las actividades que se van a auditar, cuándo serán auditadas, el tiempo estimado requerido, tomando en consideración el alcance del trabajo de auditoría planeado y la naturaleza y extensión del trabajo de auditoría realizado por otros. Los programas de trabajo deberán ser lo suficientemente flexibles para cubrir demandas imprevistas.

Los planes de contratación de empleados y los presupuestos financieros (incluyendo el número de auditores, su conocimiento, su experiencia y las disciplinas requeridas para realizar su trabajo), deberán contemplarse al elaborar los programas de trabajo de auditoría, así como las actividades administrativas, la escolaridad y el adiestramiento requeridos, la investigación sobre auditoría y los esfuerzos de desarrollo.

II.3.- Revisión Preliminar.

El primer paso en el desarrollo de la auditoría, después de la planeación, es la revisión preliminar del área de Informática. El objetivo de la revisión preliminar es el de obtener la información necesaria para que el auditor pueda tomar la decisión de cómo proceder en la auditoría, (Brandon, 2002). Al terminar la revisión preliminar el auditor puede proceder en uno de los tres caminos siguientes:

- Diseño de la auditoría. Puede haber problemas debido a la falta de competencia técnica para realizar la auditoría.
- Realizar una revisión detallada de los controles internos de los sistemas con la esperanza de que se deposite la confianza en los controles de los sistemas y de que una serie de pruebas sustantivas puedan reducir las consecuencias.
- Decidir el no confiar en los controles internos del sistema. Existen dos razones posibles para esta decisión. Primero, puede ser más eficiente desde el punto de vista de costo-beneficio el realizar pruebas sustantivas directamente. Segundo, los controles del área de Informática pueden duplicar los controles existentes en el área del usuario. El auditor puede decidir que se obtendrá un mayor costo-beneficio al dar una mayor confianza a los controles de compensación y revisar y probar mejor estos controles.

La revisión preliminar significa la recolección de evidencias por medio de entrevistas con el personal de la instalación, la observación de las actividades en la instalación y la revisión de la documentación preliminar. Las evidencias se pueden recolectar por medio de cuestionarios iniciales, o bien por medio de entrevistas, o con documentación narrativa. Se debe considerar que ésta será sólo una información inicial que permitirá elaborar el Plan de Trabajo, la cual se profundizará en el desarrollo de la auditoría.

La revisión preliminar elaborada por un auditor interno difiere de la realizada por un auditor externo en tres aspectos. En primer lugar, el auditor interno normalmente requiere de menos revisiones y trabajos, especialmente en la parte gerencial y de organización, ya que él es parte de la Organización y está familiarizado con la misma. En segundo, el auditor externo se enfoca más en las causas de las pérdidas y en los controles necesarios para justificar sus decisiones; el auditor interno tiene una amplia perspectiva, la cual incorpora en sus consideraciones sobre la eficiencia y la eficacia con la que se trabaja. En tercero, si el auditor interno supone serias debilidades en los controles internos, en lugar de proceder directamente con las pruebas sustantivas, deberá continuar con la fase de revisión detallada para señalar recomendaciones para mejorar los controles internos.

II.4.- Revisión Detallada.

Los objetivos de la fase detallada son los de obtener información necesaria para que el auditor tenga un profundo entendimiento de los controles usados dentro del área de Informática. El auditor debe decidir si debe continuar elaborando pruebas de consentimiento, con la esperanza de obtener mayor confianza por medio del sistema de control interno, o proceder directamente a la revisión con los usuarios (pruebas compensatorias), o las pruebas sustantivas. En algunos casos el auditor puede, después de hacer un análisis detallado, decidir que con los controles internos se tiene suficiente confianza, y en otros casos que los procedimientos alternos de auditoría pueden ser más apropiados, (Dorf y Bishop, 1995).

En la fase de evaluación detallada es importante para el auditor identificar las causas de las pérdidas existentes dentro de la instalación y los controles ára reducir las pérdidas y los efectos causados por éstas. Al terminar la revisión detallada el auditor debe evaluar en qué momento los controles establecidos reducen las pérdidas esperadas a un nivel aceptable. Los métodos de obtención de información al momento de la evaluación detallada son los mismos usados en la investigación preliminar, y lo único que difiere es la profundidad con que se obtiene la información y se evalúa.

Como en el caso de la investigación preliminar, se tienen diferentes formas de lograr los objetivos desde el punto de vista del auditor interno o externo. El auditor interno debe considerar las causas de las pérdidas que afectan la eficiencia y eficacia, además de evaluar por qué los controles escogidos son o no son suficientes para reducir las pérdidas esperadas a un nivel aceptable. El auditor interno debe evaluar si los controles escogidos son óptimos, si provocan un sobrecontrol, o bien si se logra un satisfactorio nivel de control usando menos controles o controles menos costosos. Si el auditor interno considera que los controles internos del sistema no son satisfactorios, en lugar de proceder directamente a revisar, a probar controles alternos o a realizar pruebas sustantivas y procedimientos, debe señalar las recomendaciones para mejorar los controles de los sistemas.

II.5.- Examen y Evaluación de la Información.

Los auditores internos deberán obtener, analizar, interpretar y documentar la información para apoyar los resultados de la auditoría. El proceso de examen y evaluación de la información es el siguiente:

- Se debe obtener la información de todos los asuntos relacionados con los objetivos y alcances de la auditoría.
- La información deberá ser suficiente, competente, relevante y útil para que proporcione bases sólidas en relación con los hallazgos y recomendaciones de la auditoría. La información suficiente significa que está basada en hechos, que es adecuada y convincente, de tal forma que una persona prudente e informada pueda llegar a las mismas conclusiones con el auditor. La información competente significa que es confiable y puede obtenerse de la mejor manera, usando las técnicas de auditoría apropiadas. La información relevante apoya los hallazgos y recomendaciones de auditoría y es consistente con los objetivos de ésta. La información útil ayuda a la Organización a lograr sus metas.
- Los procedimientos de auditoría, incluyendo el empleo de las técnicas de prueba selectivas y el muestreo estadístico, deberán ser elegidos con anterioridad, cuando esto sea posible, y ampliarse o modificarse cuando las circunstancias lo requieran.
- El proceso de recabar, analizar, interpretar y documentar la información deberá supervisarse para proporcionar una seguridad razonable de que la objetividad del auditor se mantuvo y que las metas de auditoría se cumplieron.
- Los documentos de trabajo de la auditoría deberán ser preparados por los auditores y revisados por la Gerencia de Auditoría. Estos documentos deberán registrar la información obtenida y el análisis realizado, y deben apoyar las bases de los hallazgos de auditoría y las recomendaciones que se harán.

Los auditores deberán reportar los resultados del trabajo de auditoría. El auditor deberá discutir las conclusiones y recomendaciones en los niveles apropiados de la administración antes de emitir su informe final. Los informes deberán ser objetivos, claros, concisos, constructivos y oportunos. Los informes presentarán el propósito, alcance y resultados de la auditoría y, cuando se considere apropiado, contendrán la opinión del auditor, (Fine, 1998)..

Los informes pueden incluir recomendaciones para mejorar potenciales y reconocer el trabajo satisfactorio y las medidas correctivas. Los puntos de vista de los auditados respecto a las conclusiones y recomendaciones pueden ser incluidos en el informe de auditoría.

Los auditores internos realizarán el seguimiento de las recomendaciones para asegurarse que se tomaron las acciones apropiadas sobre los hallazgos de auditoría reportados. El Director de Auditoría en Informática deberá establecer un programa para seleccionar y desarrollar los recursos, el cual debe contemplar:

- Descripciones de puestos por cada nivel de Auditoría en Informática.
- Selección de individuos calificados y competentes.
- Entrenamiento y oportunidad de capacitación profesional continua para todos y cada uno de los auditores.
- Evaluación del trabajo de cada uno de los auditores por lo menos una vez al año.
- Asesoría a los auditores en lo referente a su trabajo y a su desarrollo profesional.

El trabajo de auditoría interna y externa deberá coordinarse para asegurar la adecuada cobertura y para minimizar la duplicidad de esfuerzos. El Director de Auditoría Interna en Informática deberá establecer y mantener un programa de Control de Calidad para evaluar las operaciones del Departamento de Auditoría Interna. El propósito de este programa es proporcionar una seguridad razonable de que el trabajo de auditoría está de acuerdo con las Normas aplicables. Un Programa de Control de Calidad deberá incluir los siguientes elementos:

- Supervisión.
- Revisiones Internas.
- Revisiones Externas.

La supervisión del trabajo de los auditores en Informática deberá llevarse a cabo continuamente para asegurarse de que están trabajando de acuerdo con las Normas, Políticas y Programas de Auditoría en Informática.

Las revisiones internas deberán realizarse periódicamente por el personal del Departamento de Auditoría Interna para evaluar la calidad del trabajo de auditoría realizado. Estas revisiones deberán llevarse a cabo de la misma manera que cualquier otra auditoría. Para evaluar la calidad del trabajo de Auditoría en Informática deberán practicarse revisiones externas.

II.6.- Pruebas de Consentimiento.

El objetivo de la fase de prueba de consentimiento es el de determinar si los controles internos operan como fueron diseñados para operar. EL auditor debe determinar si los controles declarados en realidad existen y si realmente trabajan confiablemente. Además de las técnicas manuales de recolección de evidencias, muy frecuentemente el auditor debe recurrir a técnicas de recolección de información asistidas por Ordenador, para determinar la existencia y confiabilidad de los controles. Por ejemplo, para evaluar la existencia y confiabilidad de los controles de un sistema en red, se requerirá el entrara a la red y evaluar directamente al sistema.

II.7.- Pruebas de Controles del Usuario.

En algunos casos el auditor puede decidir el no contar en los controles internos dentro de las instalaciones informáticas, porque el usuario ejerce controles que compensan cualquier debilidad dentro de los controles internos de Informática. Estas pruebas que compensan las deficiencias de los controles internos se pueden realizar mediante cuestionarios, entrevistas, vistas y evaluaciones hechas directamente con los usuarios.

II.8.- Pruebas Sustantivas.

El objetivo de la fase de pruebas sustantivas es obtener evidencia suficiente que permita al auditor emitir su juicio en las conclusiones acerca de cuándo pueden ocurrir pérdidas materiales durante el procesamiento de la información, (Martin, 1994). El auditor externo expresará este juicio en forma de opinión sobre cuándo puede existir un proceso equivocado o falta de control de la información. Se pueden identificar ocho pruebas sustantivas:

- ✓ Pruebas para identificar errores en el procesamiento o de la falta de seguridad o confidencialidad.
- ✓ Pruebas para asegurar la calidad de los datos.
- ✓ Pruebas para identificar la inconsistencia de los datos.
- ✓ Pruebas para comparar con los datos o contadores físicos.
- ✓ Confirmación de datos con fuentes externas.
- ✓ Pruebas para confirmar la adecuada comunicación.

- ✓ Pruebas para determinar falta de seguridad.
- ✓ Pruebas para determinar problemas de legalidad.

Se debe cuestionar el beneficio de tener un excesivo control o bien evaluar el beneficio marginal de tener mayor control contra el costo que representa éste. Para ello es necesario evaluar el costo por falla del sistema y sus repercusiones para determinar el grado de riesgo y confianza necesarios contra el costo de implantación de controles y el costo de recuperación de la información o eliminación de las repercusiones.

El auditor debe participar en tres estados del sistema:

- Durante la fase de diseño del sistema.
- Durante la fase de operación.
- Durante la fase posterior a la auditoría.

En general, la opinión del Gerente de Informática y de la alta Gerencia consideran que el que el auditor participe en la fase de diseño disminuye la independencia del auditor, pero existen varias formas en las cuales se puede eliminar esto:

- o Aumentando los conocimientos en Informática del auditor.
- o Asignar diferentes auditores a la fase de diseño, al trabajo de auditoría y al posterior a la auditoría.
- o Crear una sección de Audioría en Informática dentro del Departamento de Auditoría Interno, especializado en Auditoría en Informática.
- o Obtener mayor soporte de la alta gerencia.

Realizar una Auditoría en Informática es un trabajo complejo. Por ello, para lograr los objetivos, el auditor necesita dividir los sistemas en una serie de subsistemas, identificar los componentes que realizan las actividades básicas de cada subsistema, evaluar la confianza de cada componente, y la de los subsistemas, y en forma agregada evaluar cada subsistema hasta llegar a una evaluación global sobre la confianza total del sistema. Esto se deberá realizar sin olvidar el postulado de Investigación de Operaciones que señala que: *" La suma de los óptimos parciales de los subsistemas no es igual al óptimo del sistema, pero nos da una buena aproximación".*

Los pasos que involucran una Auditoría en Informática son similares a aquellos que se realizan para auditar un sistema manual. Primero se realiza una investigación preliminar del Área de Informática, para lograr un entendimiento de cómo está siendo administrada la instalación y de los principales sistemas que son procesados. En segundo lugar, si el auditor determina confiar en los controles internos del sistema, se realiza una investigación detallada.

En tercero, el auditor, de acuerdo con su juicio, prueba la confianza sobre aquellos controles que son críticos. En cuarto, se realizan pruebas sustantivas de los procedimientos. Finalmente, el auditor debe dar una opinión. Después de estos pasos el auditor evalúa los controles internos del sistema y decide si debe proceder con pasos alternativos.

Durante la Auditoría en Informática deben tomarse muchas decisiones difíciles. Cada evaluación sobre la confianza de los sistemas de control interno requiere de evaluaciones complejas realizadas en forma conjunta con las evidencias obtenidas.

II.9.- Evaluación de los Sistemas de Acuerdo al Riesgo.

Una de las formas de evaluar la importancia que puede tener para la organización un determinado sistema, es considerar el riesgo que implica el que no sea utilizado adecuadamente, la pérdida de la información o bien el que sea usado por personal ajeno a la organización, (Murdic, 2001). Para evaluar el riesgo de un sistema con mayor detalle. Algunos sistemas de aplicaciones son de más alto riesgo que otros debido a que:

- Son susceptibles a diferentes tipos de pérdida económica. Por ejemplo; fraudes y desfalcos entre los cuales están los sistemas financieros. El auditor debe poner especial atención a aquellos sistemas que requieran de un adecuado control financiero. Por ejemplo; flujo de caja, inversiones, cuentas por pagar y cobrar, nómina.
- Las fallas pueden impactar grandemente a la organización. Por ejemplo; una falla en el procesamiento de la nómina puede tener como consecuencia el que se tenga una huelga.
- Interfieren con otros sistemas, y los errores generados permean a otros sistemas
- Potencialmente, alto riesgo debido a daños en la competencia. Algunos sistemas le dan a la organización un nivel competitivo muy alto dentro de un mercado. Por ejemplo; sistema de planeación estratégica. Patentes, derechos de autor, los cuales son las mayores fuentes de recursos de la organización. Otros a través de los cuales su pérdida puede destruir la imagen de la organización.
- Sistemas de tecnología de punta o avanzada. Si los sistemas utilizan tecnología avanzada o de punta. Por ejemplo; sistemas de bases de datos, sistemas distribuidos o de comunicación, tecnología sobre la cual la organización tenga muy poca experiencia o respaldo, la cual es más probable que sea una fuente de problemas de control.

- Sistemas de alto costo. Sistemas que son muy costosos de desarrollar, los cuales son frecuentemente sistemas complejos que pueden presentar muchos problemas de control.

II.10.- Investigación Preliminar.

Es necesario iniciar el trabajo de obtención de datos con un contacto preliminar que permita una primera idea global. El objetivo de este primer contacto es percibir rápidamente las estructuras fundamentales y diferencias principales entre el organismos a auditar y otras organizaciones que se hayan investigado.

La investigación preliminar debe incorporar fases de evaluación del control gerencial y del control de las aplicaciones. Durante la revisión de los controles gerenciales el auditor debe entender a la organización y las políticas y prácticas gerenciales usadas en cada uno de los niveles, dentro de la jerarquía de la instalación en que se encuentran los ordenadores. Durante la revisión de los controles de las aplicaciones, el auditor debe entender los controles ejercidos sobre el mayor tipo de transacciones que fluyen a través de los sistemas de aplicaciones más significativos dentro de la instalación de ordenadores, (Werss, 2002).

Se debe recopilar información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitudes de documentos; la finalidad es definir el objetivo y alcance des estudio, así como el programa detallado de la investigación. Se deberá observar el estado general del departamento o área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

En el caso de la Auditoria en Informática se debe comenzar la investigación preliminar con una visita al organismo, al área de informática y a los equipos de cómputo, y solicitar una serie de documentos. La investigación preliminar se debe hacer solicitando y revisando la información de cada una de las áreas, basándose en los siguientes puntos:

Administración.- Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento. La eficiencia en el Departamento de Informática sólo se puede lograr si sus objetivos están integrados con los de la Institución y si permanentemente se adapta a los posibles cambios de éstos.

Esta adaptación únicamente puede ser posible si los altos ejecutivos y los usuarios de los sistemas toman parte activa en las decisiones referentes a la dirección y utilización de los sistemas de información, y si el responsable de dicho sistemas constantemente consulta y pide asesoría y cooperación a los ejecutivos y usuarios.

Así mismo, el control de la Dirección de Informática no es posible, a menos que el personal responsable aplique la misma disciplina de trabajo y los métodos que se exigen normalmente a los usuarios. Se puede hablar de tener el control, únicamente cuando se contemplaron los objetivos, se estableció un presupuesto y se registraron correctamente los costos en el desarrollo de la aplicación, y cuando ésta contempla el nivel de servicio en términos de calidad y tiempos mínimos de entrega de resultados de la operación del ordenador.

El éxito de la Dirección de Informática dentro de una Organización depende finalmente de que todas las personas responsables adopten una actitud positiva respecto a su trabajo y evalúen constantemente la eficiencia en su propio trabajo, así como el desarrollado en su área, estableciendo metas y estándares que incrementen su productividad. La Dirección de Informática, según las diferentes áreas de la Organización, es evaluada desde diferentes puntos de vista.

Los usuarios a nivel operativo generalmente la ven como una herramienta para incrementar su eficiencia en el trabajo. Para estos usuarios, la Dirección de Informática es una función de servicio. Cada grupo de usuarios tiene su propia expectativa de este tipo y nivel de servicio, sin considerar el costo del mismo y normalmente sin tomar en cuenta las necesidades de otros grupos de usuarios.

Los altos ejecutivos consideran a la Dirección de Informática como una inversión importante, que tiene la función de participar activamente en el cumplimiento de los objetivos de la Organización. Por ello, esperan un máximo del retorno de su inversión; esperan que los recursos destinados a la Dirección de Informática proporcionen un beneficio máximo a la Organización y que ésta participe en la administración eficiente y en la minimización de los costos mediante información que permita una adecuada toma de decisiones. Los directivos, con toda la razón, consideran que la organización cada día depende más del área de Informática y consecuentemente esperan que se deba administrar lo más eficiente y eficaz posible, (Derrien, 2000).

Esencialmente, la meta principal de los administradores de la Dirección de Informática es la misma que inspira cualquier departamento de servicios: combinar un servicio adecuado con una operación económica. El problema estriba en balancear el nivel de servicios a los usuarios que siempre puede ser incrementado a costa de un incremento en el factor económico o viceversa. Para poder analizar y dimensionar la estructura a auditar se debe solicitar:

1.- A nivel Organización Total:

- Objetivos a corto y largo plazo(s).
- Manual de la Organización.
- Antecedentes o historia del organismo.
- Políticas generales.

2.- A nivel del Área de Informática:

- Objetivos a corto y largo plazo(s).
- Manual de organización del área que incluya puestos, funciones, niveles jerárquicos y tramos de mando.
- Manual de políticas, reglamentos internos y lineamientos generales.
- Número de personas y puestos en el área.

3.- Recursos Materiales y Técnicos:

- Solicitar documentos sobre los equipos, así como el número de ellos, su localización y sus características (de los equipos instalados, por instalar y programados).
- Estudios de viabilidad.
- Fechas de instalación de los equipos y planes de instalación.
- Contratos vigentes de compra, renta y servicios de mantenimiento.
- Contratos de seguros.
- Convenios que se tienen con otras instalaciones.
- Configuración de los equipos y capacidades actuales y máximas
- Configuración de equipos de comunicación (redes internas y externas) y localización de los equipos.
- Planes de expansión.
- Ubicación general de los equipos.
- Políticas de operación.
- Políticas de uso de los equipos.
- Políticas de seguridad física y prevención contra constingencias internas y externas.

4.- Sistemas:

- Descripción general de los sistemas instalados y de los que estén por instalarse, que contengan volúmenes de información.
- Manual de formas.
- Manual de procedimientos de los sistemas.
- Descripción genérica.
- Diagramas de entrada, archivos, salida.
- Fecha de instalación de los sistemas.
- Proyecto de instalación de nuevos sistemas.
- Base(s) de Datos, propietarios de la información y usuarios de la misma.

- Procedimientos y políticas en caso de desastre(s).
- Sistemas propios, rentados y adquiridos.

En el momento de hacer la planeación de la auditoría o bien en su realización, se debe evaluar que pueden presentarse cualquiera de las siguientes situaciones:

- Se solicita la información y se ve que:

- No se tiene y se necesita.
- No se tiene y no se necesita.

- Se tiene la información, pero:

- No se usa.
- Es incompleta.
- No está actualizada.
- No es la adecuada.
- Se usa, está actualizada, es la adecuada y está completa.

En el caso de que no se disponga de la información y se considere que no se necesita, se debe evaluar la causa por la que no es necesaria, ya que se puede estar solicitando un tipo de información que debido a las características del organismos no se requiera. Eso dará un parámetro muy importante para hacer una adecuada planeación de la auditoría.

En el caso de que no se tenga la información pero que sea necesaria, se debe recomendar que se elabore con las necesidades y con el uso que se le va a dar. En el caso de que se tenga la información pero que no utilice, se debe analizar porqué no se usa. El motivo puede ser que esté incompleta, que no esté actualizada, que no sea la adecuada, etcétera. Hay que analizar y definir las causas para señalar alternativas de solución, lo que lleva a la utilización de la información.

En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa; de ser así, se considerará dentro de las conclusiones de la evaluación, ya que como se dijo, la auditoría no sólo debe considerar errores, sino también señalar los aciertos. Antes de concluir esta etapa, no se olvide que el éxito del análisis crítico depende de las consideraciones siguientes:

- ✓ Estudiar hechos y no opiniones (no se toman en cuenta los rumores, ni la información sin fundamento). Investigar las causas, no los efectos.
- ✓ Atender razones, no excusas.
- ✓ No confiar en la memoria, preguntar constantemente.
- ✓ Criticar objetivamente y a fondo todos los informes y los datos recabados.

II.11.- Personal Participante.

Una de las partes más importantes en la planeación de la Auditoría en Informática, es el personal que deberá participar. En este punto no se verá el número de personas que deberán participar, ya que esto depende de las dimensiones de la Organización, de los sistemas y de los equipos; lo que se deberá considerar son las características del personal que habrá de participar en la auditoría.

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervenga esté debidamente capacitado, que tenga un alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo. Con estas bases se debe considerar los conocimientos, la práctica profesional y la capacitación que debe tener el personal que intervendrá en la auditoría.

En primer lugar, se debe pensar que hay personal asignado por la Organización, que deba tener el suficiente nivel para poder coordinador el desarrollo de la auditoría, proporcionarnos toda la información que se solicite y programar las reuniones y entrevistas requeridas. Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, será casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información, o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se está solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la Dirección de Informática, sino también el del usuario del sistema. Para completar el grupo, como colaboradores directos en la realización de la auditoría, se deben tener personas con las siguientes características:

- Técnico en Informática.
- Conocimientos de Administración, Contaduría y Finanzas.
- Experiencia en el área de Informática.
- Experiencia en operación y análisis de sistemas.
- Conocimientos y experiencia en psicología industrial.
- Conocimientos de los sistemas operativos, bases de datos, redes y comunicaciones, dependiendo del área y características a auditar.
- Conocimientos de los sistemas más importantes.

En el caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, comunicaciones, etcétera. Lo anterior no significa que una sola persona deba tener los conocimientos y experiencias señaladas, pero sí que deben intervenir una o varias personas con las características apuntadas.

Una vez planeada la forma de llevar a cabo la auditoría, se estará en posibilidad de presentar la carta (convenio de servicios profesionales en el caso de auditores externos), y el plan de trabajo. La carta convenio es un compromiso que el auditor dirige a su cliente para su confirmación de aceptación. En ella se especifican el objetivo y alcance de la auditoría, las limitaciones y la colaboración necesaria, el grado de responsabilidad y los informes que se han de entregar.

Una vez que se ha hecho la planeación, se puede utilizar el formato señalado en la Figura II.1, el cual servirá para resumir el Plan de Trabajo de la Auditoría. Este formato de programa servirá de base para llevar un adecuado control del desarrollo de la misma. En él figuran el organismo, la fecha de formulación, las fases y subfases que comprenden la descripción de la actividad, el número de personas participantes, las fechas estimadas de inicio y terminación, el número de días hábiles y el número de días-hombre estimados.

El control del avance de la auditoría se puede llevar mediante el formato de la Figura II.2, el cual permite cumplir con los procedimientos de control y asegurarse que el trabajo se está llevando a cabo de acuerdo con el programa de auditoría, con los recursos estimados y en el tiempo señalado en la planeación. El hecho de contar con la información del avance permite que el trabajo elaborado pueda ser revisado por cualquiera de los asistentes. Como ejemplo de propuesta de Auditoría en Informática, véase la Figura II.3, y como ejemplo de contrato de Auditoría en Informática consúltese la Figura II.4, (Echenique, 2001).

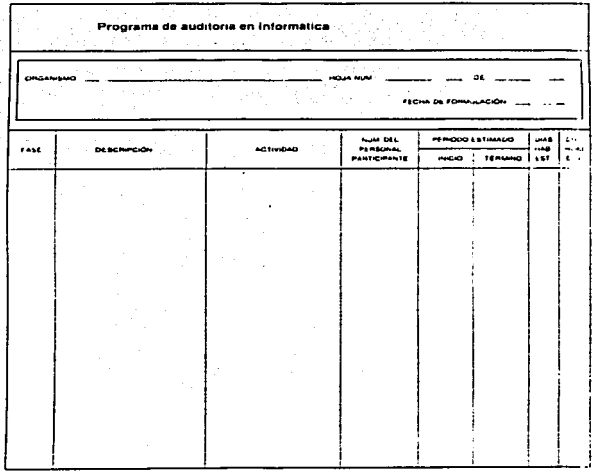


Figura II.1.- Programa de Auditoria en Informática.

Avance del cumplimiento del programa de auditoria en informatica

ORGANISMO _____ NUM _____ HOJA NUM _____ DE _____

PERIODO QUE REPORTA _____

FASE	SITUACION DE LA AUDITORIA			PERIODO REAL DE LA AUDITORIA		DIAS REALES UTILIZADOS	VARIACION DE AVANCE	DIAS PROGRAMADOS EST	EXPLICACION DE LAS VARIACIONES EN RELACION CON LO PROGRAMADO
	NO INICIADA	EN PROCESO	TERMINADA	INICIADA	TERMINADA				

Figura II.2.- Avance del Cumplimiento del Programa de Auditoría en Informática.

Ejemplo de propuesta de servicios de auditoria en informatica

I. ANTECEDENTES

(Anotar los antecedentes especificos del proyecto de auditoría.)

II. OBJETIVOS DE LA AUDITORIA EN INFORMATICA

(Anotar el objetivo especifico de la auditoría.)

III. ALCANCES DEL PROYECTO

El alcance del proyecto comprende:

1. Evaluacion de la direccion de informatica en lo que corresponde a:
   - Su organización.
   - Funciones.
   - Objetivos.
   - Estructura.
   - Recursos humanos.
   - Normas y politicas.
   - Capacitacion.
   - Planes de trabajo.
   - Controles.
   - Estandares.
   - Condiciones de trabajo.
   - Situacion presupuestal y financiera.
2. Evaluacion de los sistemas:
   - Evaluacion de los diferentes sistemas en operacion (flujo, procedimientos, documentacion, organizacion de archivos, estandares de programacion, controles, utilizacion de los sistemas, opiniones de los usuarios).
   - Evaluación de avances de los sistemas en desarrollo y congruencia con el diseño general, control de proyectos, modularidad de los sistemas.
   - Seguridad lógica de los sistemas, confidencialidad y respaldos.
   - Derechos de autor y secretos industriales, de los sistemas propios y los utilizados por la organización.
   - Evaluacion de las bases de datos.
3. Evaluacion de los equipos:
   - Adquisición
   - Estandarización
   - Costos
   - Revisión proyectos de adquisicion.
   - Almacenamiento.
   - Comunicacion.

Figura II.3.- Ejemplo de Propuesta de Servicios de Auditoría en Informática.

- Redes
- Equipos adicionales.

4. Evaluacion de la seguridad

- Seguridad logica y confidencialidad.
- Seguridad en el personal.
- Seguridad fisica.
- Seguridad contra virus
- Seguros
- Seguridad en la utilizacion de los equipos.
- Seguridad en la restauracion de los equipos y de los sistemas.
- Plan de contingencia y procedimientos en caso de desastre.

IV. METODOLOGIA

La metodologia de investigacion a utilizar en el proyecto se presenta a continuacion.

1. Para la evaluacion de la direccion de informatica se llevaran a cabo las siguientes actividades:

   - Solicitud de los manuales administrativos, organizacion, funciones, planes, politicas, estandares utilizados y programas de trabajo.
   - Solicitud de costos y presupuestos de informatica.
   - Elaboracion de un cuestionario para la evaluacion de la direccion.
   - Aplicacion del cuestionario al personal, y realizacion de entrevistas.
   - Entrevistas a lideres de proyectos y a usuarios mas relevantes de la direccion de informatica.
   - Analisis y evaluacion de la informacion.
   - Elaboracion del informe.

2. Para la evaluacion de los sistemas tanto en operacion como en desarrollo se llevaran a cabo las siguientes actividades:

   - Estudios de viabilidad y costo/beneficio.
   - Solicitud del analisis y diseño de los sistemas en operacion y en desarrollo.
   - Solicitud de documentacion de los sistemas en operacion (manuales tecnicos, de operación, de usuario, diseños).
   - Solicitud del plan de trabajo.
   - Solicitud de contratos de compra o renta de software.
   - Solicitud de licencias y derechos de autor.
   - Plan de contingencia y recuperacion en casos de desastre.
   - Recopilacion y analisis de los procedimientos administrativos de cada sistema.
   - Analisis de bases de datos.

Figura II.3.- Ejemplo de Propuesta de Servicios de Auditoría en Informática.

- Analisis de la seguridad logica y confidencialidad.
- Evaluacion de los proyectos en desarrollo, prioridades y personal asignado.
- Evaluacion de la participacion de auditoria interna.
- Evaluacion de controles.
- Evaluacion de las licencias, la obtencion de derechos de autor y de la confidencialidad de la informacion.
- Entrevistas con usuarios de los sistemas.
- Evaluacion directa de la informacion obtenida contra las necesidades y requerimientos de los usuarios.
- Analisis objetivo de la estructuracion y flujo de los programas.
- Analisis y evaluacion de la informacion compilada.
- Elaboracion de informe.

3. Para la evaluacion de los equipos se llevarán a cabo las siguientes actividades:

- Solicitud de los estudios de viabilidad, costo/beneficio y caracteristicas de los equipos actuales, proyectos sobre adquisicion o ampliacion de equipo y su actualizacion.
- Solicitud de contratos de compra o renta de los equipos.
- Solicitud de contratos de mantenimiento de los equipos.
- Solicitud de contratos y convenios de respaldo.
- Solicitud de contratos de seguros.
- Bitácoras de los equipos.
- Elaboracion de un cuestionario sobre la utilizacion de equipos, archivos, unidades de entrada/salida, equipos perifericos, y su seguridad.
- Visita a las instalaciones y a los lugares de almacenamiento de archivos magneticos.
- Visita tecnica de comprobacion de seguridad fisica y logica de las instalaciones.
- Evaluacion tecnica del sistema electrico y ambiental de los equipos, del local utilizado y en general de las instalaciones.
- Evaluacion de los sistemas de seguridad de acceso.
- Evaluacion de la informacion recopilada, obtencion de graficas, porcentajes de utilización de los equipos y su justificacion.
- Elaboracion de informe.

4. Elaboracion del informe final, presentacion y discusion del mismo, y presentacion de conclusiones y recomendaciones.

V. TIEMPO Y COSTO

(Poner el tiempo en que se realizara el proyecto, de preferencia indicando el tiempo de cada una de las etapas, el costo del mismo, que incluya el personal participante en la auditoria y sus caracteristicas, y la forma de pago.)

Figura II.3.- Ejemplo de Propuesta de Servicios de Auditoria en Informática.

Ejemplo de contrato de auditoria en informatica

Contrato de prestacion de servicios profesionales de auditoria en informatica que celebran por una parte _____, representado por _____ en su caracter de _____ y que en lo sucesivo se denominara "el cliente", por otra parte _____, representada por _____ a quien se denominara "el auditor", de conformidad con las declaraciones y clausulas siguientes:

DECLARACIONES

I. El cliente declara:

a) Que es una _____

b) Que esta representado para este acto por _____ y que tiene como su domicilio _____

c) Que requiere obtener servicios de auditoria en informatica, por lo que ha decidido contratar los servicios del auditor.

II. Declara el auditor:

a) Que es una sociedad anonima, constituida y existente de acuerdo con las leyes y que dentro de sus objetivos primordiales esta el de prestar auditoria en informatica _____

b) Que esta constituida legalmente segun escritura numero _____ de fecha _____ ante el notario publico num. _____ del _____ Lic. _____

c) Que señala como su domicilio _____

III. Declaran ambas partes:

a) Que habiendo llegado a un acuerdo sobre lo antes mencionado, lo formalizan otorgando el presente contrato que se contiene en las siguientes:

CLAUSULAS

Primera. Objeto
El auditor se obliga a prestar al cliente los servicios de auditoria en informatica para llevar a cabo la evaluacion de la direccion de informatica del cliente, que se detallan en la propuesta de servicios anexa que, firmada por las partes, forma parte integrante del contrato.

Figura II.4.- Ejemplo de Contrato de Auditoria Informática.

Segunda. Alcance del trabajo
El alcance de los trabajos que llevará a cabo el auditor interno dentro de este contrato son:

a) Evaluaciones de la dirección de informática en lo que corresponde a:

- Su organización.
- Funciones.
- Estructura.
- Cumplimiento de los objetivos.
- Recursos humanos.
- Normas y políticas.
- Capacitación.
- Planes de trabajo.
- Controles.
- Estándares.
- Condiciones de trabajo.
- Situación presupuestal y financiera.

b) Evaluación de los sistemas:

- Evaluación de los diferentes sistemas en operación (flujo, procedimientos, documentación, organización de archivos, estándares de programación, controles, utilización de los sistemas).
- Opiniones de los usuarios.
- Evaluación de avances de los sistemas en desarrollo y congruencia con el diseño general, control de proyectos, modularidad de los sistemas.
- Evaluación de prioridades y recursos asignados (humanos y equipos de cómputo).
- Seguridad lógica de los sistemas, confidencialidad y respaldos.
- Derechos de autor y secretos industriales, de los sistemas propios y los utilizados por la organización.
- Evaluación de las bases de datos.

c) Evaluación de los equipos:

- Adquisición, estudios de viabilidad y costo-beneficio.
- Capacidades.
- Utilización.
- Estandarización.
- Controles.
- Nuevos proyectos de adquisición.
- Almacenamiento.
- Comunicación.
- Redes.
- Equipos adicionales.
- Respaldos de equipos.

Figura II.4.- Ejemplo de Contrato de Auditoría Informática.

- Contratos de compra, renta o renta con opcion a compra
- Planes y proyecciones de adquisicion de nuevos equipos.
- Mantenimientos.

d) Evaluacion de la seguridad:

- Seguridad logica y confidencialidad.
- Seguridad en el personal.
- Seguridad fisica
- Seguridad contra virus
- Seguros
- Seguridad en la utilizacion de los equipos.
- Seguridad en la restauracion de los equipos y de los sistemas.
- Plan de contingencia y procedimientos en caso de desastre.

e) Elaboracion de informes que contengan conclusiones y recomendaciones por cada uno de los trabajos señalados en los incisos *a, b, c, d* de esta clausula.

Tercera. Programa de trabajo
El cliente y el auditor convienen en desarrollar en forma conjunta un programa de trabajo en el que se determinen con precision las actividades a realizar por cada una de las partes, los responsables de llevarlas a cabo y las fechas de realizacion.

Cuarta. Supervision
El cliente o quien designe tendra derecho a supervisar los trabajos que se le han encomendado al auditor dentro de este contrato y a dar por escrito las instrucciones que estime convenientes.

Quinta. Coordinacion de los trabajos
El cliente designara por parte de la organizacion a un coordinador del proyecto, quien sera el responsable de coordinar la recopilacion de la informacion que solicite el auditor, y de que las reuniones y entrevistas establecidas en el programa de trabajo se lleven a cabo en las fechas establecidas.

Sexta. Horario de trabajo
El personal del auditor dedicara el tiempo necesario para cumplir satisfactoriamente con los trabajos materia de la celebracion de este contrato, de acuerdo al programa de trabajo convenido por ambas partes, y gozara de libertad fuera del tiempo destinado al cumplimiento de las actividades, por lo que no estara sujeto a horarios y jornadas determinadas.

Septima. Personal asignado
El auditor designara para el desarrollo de los trabajos objeto de este contrato a socios del despacho, quienes, cuando consideren necesario, incorporaran personal tecnico capacitado de que dispone la firma, en el numero que se requieran y de acuerdo a los trabajos a realizar

Figura II.4.- Ejemplo de Contrato de Auditoría Informática.

Octava. Relacion laboral
El personal del auditor no tendra ninguna relacion laboral con el cliente y queda expresamente estipulado que este contrato se suscribe en atencion a que el auditor en ningun momento se considera intermediario del cliente respecto al personal que ocupe para dar cumplimiento de las obligaciones que se deriven de las relaciones entre el y su personal, y que exime al cliente de cualquier responsabilidad que a este respecto existiere.

Novena. Plazo de trabajo
El auditor se obliga a terminar los trabajos señalados en la clausula segunda de este contrato en _____ dias habiles despues de la fecha en que se firme el contrato y sea cobrado el anticipo correspondiente. El tiempo estimado para la terminacion de los trabajos esta con relacion a la oportunidad con que el cliente entregue los documentos requeridos por el auditor y al cumplimiento de las fechas estipuladas en el programa de trabajo aprobado por las partes, por lo que cualquier retraso ocasionado por parte del personal del cliente o de usuarios de los sistemas repercutira en el plazo estipulado, el cual debera incrementarse de acuerdo a las nuevas fechas establecidas en el programa de trabajo, sin perjuicio alguno para el auditor.

Decima. Honorarios
El cliente pagará al auditor por los trabajos objeto del presente contrato, honorarios por la cantidad de _____ mas el impuesto al valor agregado correspondiente. La forma de pago sera la siguiente:

a) _____% a la firma del contrato.
b) _____% a los _____ dias habiles despues de iniciados los trabajos.
c) _____% a la terminación de los trabajos y presentacion del informe final.

Undecima. Alcance de los honorarios
El importe señalado en la clausula decima compensara al auditor por sueldos, honorarios, organizacion y dirección tecnica propia de los servicios de auditoria, prestaciones sociales y laborales de su personal.

Duodecima. Incremento de honorarios
En caso de que se tenga un retraso debido a la falta de entrega de información, demora o cancelacion de las reuniones, o cualquier otra causa imputable al cliente, este contrato se incrementará en forma proporcional al retraso y se señalará el incremento de comun acuerdo.

Decimotercera. Trabajos adicionales
De ser necesaria alguna adicion a los alcances o productos del presente contrato, las partes celebrarán por separado un convenio que formara parte

Figura II.4.- Ejemplo de Contrato de Auditoria Informática.

integrante de este instrumento y en forma conjunta se acordara el nuevo costo.

Decimocuarta. Viaticos y pasajes
El importe de los viaticos y pasajes en que incurra el auditor en el traslado, hospedaje y alimentación que requieran durante su permanencia en la ciudad de _____, como consecuencia de los trabajos objeto de este contrato, sera por cuenta del cliente.

Decimoquinta. Gastos generales
Los gastos de fotocopiado y dibujo que se produzcan con motivo de este contrato correran por cuenta del cliente.

Decimosexta. Causas de rescision
Seran causa de rescision del presente contrato la violacion o incumplimiento de cualquiera de las clausulas de este contrato.

Decimoseptima. Jurisdiccion
Todo lo no previsto en este contrato se regira por las disposiciones relativas, contenidas en el Código Civil del _____ y, en caso de controversia para su interpretacion y cumplimiento, las partes se someten a la jurisdiccion de los tribunales federales, renunciando al fuero que les pueda corresponder en razon de su domicilio presente o futuro.

Enteradas las partes del contenido y alcance legal de este contrato, lo rubrican y firman de conformidad, en original y tres copias, en la ciudad de _____, el dia _____

EL CLIENTE

EL AUDITOR

Figura II.4.- Ejemplo de Contrato de Auditoría Informática.

CAPÍTULO III.

EVALUACIÓN DE LOS SISTEMAS QUE REQUIERE LA AUDITORÍA INFORMÁTICA.

III.1.- Evaluación de Sistemas.

Existen diversas formas por medio de las cuales las organizaciones pueden contar con los paquetes y programas *("Software")* necesario para cumplir con sus requerimientos; entre ellas se encuentran:

1.- Elaborado por el usuario o bien un *"software"* **comercial.**- El que el usuario elabore un determinado *"software"* tiene las siguientes ventajas: normalmente es desarrollado para cubrir todas las necesidades del usuario; puede ser modificado de acuerdo a las necesidades de la Organización; contiene sistemas de seguridad propios. Aunque tiene estas desventajas: es más costoso; su tiempo de implantación es más largo, su mantenimiento y actualización, normalmente no se hacen sobre una base periódica.

2.- *"Software"* **compartido o regalado.**- Normalmente se trata de un *"software"* sencillo elaborado para ordenadores personales, que puede ser conseguido a bajo costo vía Internet. El peligro de este tipo de *"software"* es que no puede cumplir con todas las necesidades, además de que se debe tener cuidado con los programas pirata o con los virus.

Se debe considerar la librería de programas de aplicación. Sin importar la forma de desarrollo, los programas siempre son escritos para correr en un determinado Sistema Operativo. Un elemento importante del sistema operativo es la cantidad y diversidad de programas de aplicación que son escritas en él, lo cual se conoce como la librería de programas de aplicación. Es importante tomar en cuenta el sistema operativo, ya que puede ser un tipo de sistema operativo conocido como "propietario", el cual sólo puede ser usado en máquinas de un determinado proveedor.

3.- *"Software"* **Transportable** *(portability)*.- Se considera que un *"software"* es portable o transportable cuando:

a). Tiene diferentes versiones para diferentes sistemas operativos.

b). Cuando puede cambiarse entre dos o más sistemas operativos.
c). Cuando puede ser fácilmente convertido de un sistema operativo a otro.

Un *"software"* que es transportable permite, aparentemente, usar el mismo programa de aplicación sin importar el sistema computacional. Se puede usar en un gran equipo de cómputo *(mainframe)* o en un miniordenador, o cambiar entre diferentes tipos de miniordenadores. Una Organización que obtiene un *"software"* que tiene diferentes versiones, pero que en esencia es el mismo, lo cual significa que es transportable, ahorra tiempo en entrenamiento y en personal, y permite el que fácilmente se mueva de un trabajo a otro o bien en diferentes lugares.

4.- Un solo usuario o multiusuario.- Como en el caso de los sistemas operativos, los programas de aplicación pueden ser para un solo usuario o para una variedad de usuarios.

5.- Categorización del *"software"* de aplicación por usuario.- El *"software"* puede ser catalogado como: de propósitos generales, de funciones específicas o específico de la industria.

6.- *"Software"* a la medida de la oficina.- El *"software"* comercial puede ser vendido, o bien puede ser elaborado internamente como paquetes individuales o como paquetes integrales y compatibles que son diseñados para trabajar en conjunto. Por ejemplo, un paquete elaborado en COBOL, o una Hoja de Cálculo, pueden ser diseñados para trabajar sólo con un determinado Sistema Operativo. Los paquetes individuales pueden ocasionar muchos problemas, ya que por ejemplo se puede tener un magnífico paquete de presupuestos que sea incompatible con el paquete de contabilidad.

Si dos paquetes son diseñados en forma individual por dos diferentes compañías, es muy probable que no sean compatibles, lo cual puede repercutir en aumento de tiempo, costo y entrenamiento. Un *"software"* que es compatible e integrado permite que sus menús, apuntadores, comandos y ayudas sean iguales y que las salidas del sistema sean compatibles. El usar paquetes de *"software"* compatible, tiene grandes beneficios, aunque puede tener el inconveniente de que no todos los paquetes cumplan con los requerimientos de los usuarios, (Gratton, 1998)..

Al desarrollar un determinado sistema se debe cuidar si habrá necesidad de adquirir sistemas o lenguajes propiedad de una Compañía, que para su utilización se requiera de una licencia específica, lo cual puede ser muy costoso, o bien "casarnos" con un determinado proveedor, lo cual puede ser conveniente pero se requiere de una evaluación muy detallada. La elaboración o adquisición de sistemas debe evaluarse con mucho detalle, para lo cual se debe revisar desde la planeación y elaboración de los sistemas hasta su desarrollo e implementación. Se deberá evaluar si:

- Existen realmente sistemas entrelazados como un todo o bien si existen programas aislados.
- Existe un plan estratégico para la elaboración de los sistemas o bien, si se están elaborando sin el adecuado señalamiento de prioridades y de objetivos.
- Los recursos son los adecuados y si se están utilizando en forma eficaz y eficiente.

El Plan Estratégico deberá establecer los servicios que se prestarán en un futuro, contestando preguntas como las siguientes:

- ¿Cuáles servicios se implantarán?
- ¿ Cuándo se pondrán a disposición de los usuarios?
- ¿Qué características tendrán?
- ¿Cuántos recursos se requerirán?

La estrategia de desarrollo deberá establecer las nuevas aplicaciones y recursos que proporcionará la Dirección de Informática y la arquitectura en que estarán fundamentados:

- ¿Qué aplicaciones serán desarrolladas y cuándo?
- ¿Qué tipo de archivos se desarrollarán y cuándo?
- ¿Qué bases de datos serán desarrolladas y cuándo?
- ¿Qué lenguajes se utilizarán y en qué *"software"*?
- ¿Qué tecnología será utilizada y cuándo se implantará?
- ¿Cuántos recursos se requerirán aproximadamente?
- ¿Cuál es aproximadamente el monto de la inversión en arquitectura de sistemas y en paquetes y programas?

En lo referente a la consulta a los usuarios, el plan estratégico debe definir los requerimientos de información de la Organización:

- ¿Qué estudios van a ser realizados al respecto?
- ¿Qué metodología se utilizará para dichos estudios?
- ¿Quién administrará y realizará estos estudios?

En el área de auditoría interna debe evaluarse cuál ha sido la participación del auditor y los controles establecidos. Por último, el Plan Estratégico determina la planeación de los recursos.

- ¿Contempla el plan estratégico las ventajas de la nueva tecnología?
- ¿Cuáles serán los conocimientos requeridos por los recursos humanos planeados?
- ¿Se contemplan en la estructura organizacional los nuevos niveles jerárquicos requeridos por el plan estratégico?

❖ ¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios?

El proceso de planeación de sistemas deberá asegurarse de que todos los recursos requeridos estén claramente identificados en el plan de desarrollo de aplicaciones y datos. Estos recursos (*"hardware"*, *"software"* y comunicaciones) deberán ser compatibles con la estrategia de la arquitectura de la tecnología con que se cuenta actualmente.

Para identificar los problemas de los sistemas primero se debe detectar los síntomas, los cuales son un reflejo del área problemática; después de analizar los síntomas se podrá definir y detectar las causas, parte medular de la auditoría. Se deben reunir todos los síntomas y distinguirlos antes de señalar las causas, evitando tomar los síntomas como causas y dejando fuera todo lo que sean rumores sin fundamento. Los sistemas deben ser evaluados de acuerdo con el ciclo de vida que normalmente siguen. Para ello, se recomiendan los siguientes pasos:

A). Definición del problema y requerimientos del usuario. Examinar y evaluar los problemas y características del sistema actual, sea manual, mecánico o electrónico, así como los requerimientos por parte del usuario.

B). Estudio de Factibilidad:

- Desarrollo de los objetivos y del modelo lógico del sistema propuesto.
- Análisis preliminar de las diferentes alternativas, incluyendo el estudio de factibilidad técnico y económico de cada alternativa.
- Desarrollo de recomendaciones para el proyecto de sistema, incluyendo los tiempos y costos del proyecto.

C). Diseño General y Análisis del Sistema:

- ✓ Estudio detallado del sistema actual, incluyendo los procedimientos, diagramas de flujo, métodos de trabajo, organización y control.
- ✓ Desarrollo del modelo lógico del sistema actual.

D). Diseño del Sistema:

- Desarrollo de los objetivos para el sistema propuesto
- Desarrollo del modelo lógico del sistema propuesto, incluyendo la definición lógica de los procesos, diccionario lógico de datos y diseño lógico de las bases de datos.
- Evaluación de las diferentes opciones de diseño.
- Desarrollo del análisis costo-beneficio para evaluar las implicaciones económicas de cada alternativa.

E). Diseño Detallado:

- Desarrollo de las especificaciones para el sistema físico, incluyendo el diseño de reportes, archivos, entradas, pantallas y formas.
- Diseño de las especificaciones del programa.
- Diseño de las implantación y el tiempo y forma de llevar a cabo las pruebas.

F). Implementación y Desarrollo Físico:

- Codificación y documentación del programa.
- Evaluación y selección del equipo de cómputo.
- Desarrollo de sistemas de auditoria, control y seguridad, y desarrollo de los procedimientos de prueba.
- Desarrollo de los programas de entrenamiento.

G). Pruebas del Sistema, Evaluación y Aceptación por parte del Usuario y de Contraloría Interna:

- Modificaciones y adecuaciones.
- Instalaciones.
- Carga de datos.

H). Soporte cotidiano, cambios y mejoras al sistema. Después de esto, se vuelve nuevamente al ciclo inicial, el cual a su vez debe comenzar con el estudio de factibilidad.

También se debe evaluar que un error o corrección en el momento del diseño lógico es de fácil solución y bajo costo, pero que los errores o modificaciones entre más adelantado esté el desarrollo del sistema son más costosos y de más difícil implantación. Hay ocasiones en que un sistema en su fase de implantación tiene tantas modificaciones, que es preferible hacer uno nuevo, en lugar de usar el diseñado con demasiadas modificaciones.

La primera etapa a evaluar en el sistema es el estudio de factibilidad, el cual debe analizar si el sistema es susceptible de realizarse, cuál es su relación beneficio-costo y si es conductualmente favorable. Se deberá solicitar el estudio de factibilidad de los diferentes sistemas que se encuentren en operación, así como de los que estén en la fase de análisis para evaluar:

- La disponibilidad y características del equipo.
- Los sistemas operativos y los lenguajes disponibles.
- Las necesidades de los usuarios.
- Las formas de utilización de los sistemas.
- El costo y los beneficios que reportará el sistema.
- El efecto que producirá en quienes lo usarán.
- El efecto que éstos tendrán sobre el sistema.
- La congruencia de los diferentes sistemas.

- ❖ La congruencia entre los sistemas y la organización
- ❖ Si están definidos los procesos administrativos, la normatividad y las políticas para la utilización de los sistemas.
- ❖ Su seguridad y confidencialidad.

En el caso de los sistema que estén funcionando, se deberá comprobar si existe el estudio de factibilidad con los puntos señalados, y comparar con la realidad lo especificado en el estudio de factibilidad. Por ejemplo, en un sistema que el estudio de factibilidad señaló determinado costo y una serie de beneficios de acuerdo con las necesidades del usuario, debemos comparar cuál fue costo real y evaluar si se satisficieron las necesidades indicadas como beneficios del sistema.

Para investigar el costo de un sistema se debe considerar, con una exactitud razonable, el costo de los programas, el uso de los equipos (compilaciones, programas, pruebas, paralelos), el tiempo, el personal y la operación. En la práctica, se debe de considerar los costos directos, indirectos y de operación involucrados en un sistema, para poderlos comparar con los beneficios obtenidos.

Los beneficios que justifican el desarrollo de un sistema pueden ser el ahorro en los costos de operación, la reducción del tiempo de proceso de un sistema, una mayor exactitud, un mejor servicio, una mejoría en los procedimientos de control, una mayor confiabilidad y seguridad, una mejor comunicación y en forma más eficiente. Entre los problemas más comunes en los siguientes están los siguientes:

- Falta de estándares en el desarrollo, en el análisis y en la programación.
- Falta de participación y de revisión por parte de la alta gerencia.
- Falta de participación de los usuarios.
- Inadecuada especificación del sistema al momento de hacer el diseño detallado.
- Deficiente análisis costo-beneficio.
- Nueva tecnología no usada o usada correctamente.
- Inexperiencia por parte del personal de análisis y del de programación.
- Diseño deficiente.
- Proyección pobre de la forma en que se realizará el sistema.
- Control débil o falta de control sobre las fases de elaboración del sistema y sobre el sistema en sí.
- Problemas de auditoría (poca participación de auditoría interna en el momento del diseño del sistema).
- Inadecuados procedimientos de seguridad, de recuperación y de archivos.
- Falta de integración de los sistemas (elaboración de sistemas aislados o programas que no están unidos como sistemas).
- Documentación inadecuada o inexistente.

- Dificultad de dar mantenimiento al sistema, principalmente por falta de documentación o por excesivos cambios y modificaciones hechos al sistema.
- Problemas en la conversión e implementación.
- Procedimientos incorrectos o no autorizados.

III.2.- Evaluación del Análisis.

En esta etapa se evaluarán las políticas, procedimientos y Normas que se tienen para llevar a cabo el análisis, (Fantinatti, 2000). Se deberá evaluar la planeación de las aplicaciones que pueden provenir de cuatro fuentes principales:

- La planeación estratégica: agrupando las aplicaciones en conjuntos relacionados entre sí y no como programas aislados. Las aplicaciones deben comprender todos los sistemas que puedan ser desarrollados en la organización, independientemente de los recursos que impliquen su desarrollo y justificación en el momento de la planeación.
- Los requerimientos de los usuarios.
- El inventario de sistemas en proceso al recopilar la información de los cambios que han sido solicitados, sin importar si se efectuaron o se registraron.
- Los requerimientos de la organización y de los usuarios.

La situación de una aplicación puede ser alguna de las siguientes:

- Planeada para ser desarrollada en el futuro.
- En desarrollo.
- En proceso, pero con modificaciones en desarrollo.
- En proceso con problemas detectados.
- En proceso sin problemas.
- En proceso esporádicamente.

Se deberá documentar detalladamente la fuente que generó la necesidad de la aplicación. La primera parte será evaluar la forma en que se encuentran especificadas las políticas, los procedimientos y los estándares de análisis, si es que se cumplen y si son adecuados para la Organización. Es importante revisar la situación e que se encuentran los manuales de análisis y ver si están acordes con las necesidades de la Organización. En algunas ocasiones se tiene un microordenador con sistemas sumamente sencillos y se solicita que se lleva a cabo una serie de análisis que después hay que plasmar en documentos señalados en los estándares, lo cual hacer que esta fase sea muy compleja y costosa.

Los sistemas y su documentación deben estar acordes con las características y necesidades de una Organización específica; no se deberá tener la misma documentación para un sistema que se va a usar en ordenadores personales, el cual debe de ser documentado en forma más sencilla (el usuario no necesariamente debe de saber de computación) que un sistema en red. También deben de existir diferentes niveles de documentación (documentación para usuarios, para responsables de la información técnica).

Se debe evaluar la obtención de datos sobre la operación, el flujo, el nivel, la jerarquía de la información que se tendrá a través del sistema, así como sus límites e interfases con otros sistemas. Se ha de comparar los objetivos de los sistemas desarrollados con las operaciones actuales, para ver si el estudio de la ejecución deseada corresponde al actual.

La Auditoría en Informática debe evaluar los documentos y registros usados en la elaboración del sistema, así como todas las salidas (pantallas, las cuales deben tener una estructura "amigable") y reportes, la descripción de las actividades de flujo de la información y de procedimientos, los archivos almacenados, las bases de datos, su uso y su relación con otros archivos y sistemas, su frecuencia de acceso, su conservación, su seguridad y control, la documentación propuesta, las entradas y salidas del sistema y los documentos fuente a usarse. Dentro del estudio de los sistemas en uso se deberá solicitar:

- Manual de usuario.
- Descripción de flujo de información.
- Descripción y distribución de información.
- Manual de formas.
- Manual de reportes.
- Lista de archivos y especificación.
- Definición de Base(s) de Datos.
- Definición de Redes.

Con la información obtenida se puede dar respuesta a las siguientes preguntas:

¿Se está ejecutando en forma correcta y eficiente el proceso de información?

¿Puede ser simplificado para mejorar su aprovechamiento?

¿Se debe tener una mayor interacción con otros sistemas?

¿Se tiene propuesto un adecuado control y seguridad sobre el sistema?

¿Está en el análisis la documentación adecuada?

¿Se debe usar otro tipo de técnicas o de disposición (redes, bases de datos)?

¿Los informes de salida son confiables y adecuados?

¿Las pantallas y el sistema son amigables?

III.3.- Análisis y Diseño Estructurado.

El mayor objetivo del análisis y diseño estructurado es determinar los requerimientos exactos, de tal forma que se diseñe el sistema correcto. El diseño estructurado emplea una serie de herramientas gráficas y técnicas que permitan el análisis de tal forma que sea posible conocer errores antes de que ocurran. Un error que ocurre durante la operación puede tener un costo de 30 a 90% mientras que en la fase de aceptación puede tener un costo de 5 a 10% en la fase de pruebas del diseño, de 4 a 7% en la codificación, de 5% en la de diseño de sistemas de 3 a 6% y en la de análisis de 1 a 4% por lo cual es muy conveniente que los errores sean detectados y eliminados en las fases iniciales, (Jalife, 2002).

En el caso de los sistemas tradicionales la información puede estar incompleta, no actualizada o simplemente imprecisa, y estos problemas puede que no sea detectados, mientras que en la programación estructurada el analista recolecta información sobre procedimientos actuales, flujos de información, procesos de toma de decisiones y reportes, y así construye un modelo lógico de la situación actual, usando herramientas conocidas como diagramas lógicos de flujo de datos.

El diagrama de flujo es muy útil porque detecta los procesos, los requerimientos de información, el flujo de información, y provee un modelo gráfico del sistema actual, que puede ser utilizado para detectar mejoras y desarrollar los objetivos del nuevo sistema.

Las modificaciones mayores en los procedimientos actuales, necesidades de información y de los procesos de toma de decisiones, las cuales son necesarias para lograr los objetivos, son construidas dentro del nuevo modelo lógico y son descritas gráficamente dentro de la propuesta del diagrama lógico de flujo del nuevo sistema.

El diagrama lógico de flujo de datos del sistema propuesto se convierte en la base para desarrollar y evaluar las diferentes alternativas de diseño para el nuevo sistema. Las alternativas de diseño pueden incluir las bases para el ordenador principal (*batch*), para el sistema en línea o distribuido, para los ordenadores dedicados o miniordenadores, y para el rango de *"software"* que soporte estas configuraciones, incluyendo el desarrollo de *"software"*, los paquetes de programas, usando lenguajes de cuarta generación, las bases de datos y sus caracteristicas. Una vez que son seleccionadas estas alternativas se puede comenzar el diseño detallado y la implantación del sistema. Este proceso incolucra el diseño de las salidas y de las entradas, los requerimientos de archivos y los procedimientos de control.

III.4.- Evaluación del Diseño Lógico del Sistema.

En esta etapa se deberán analizar las especificaciones del sistema:

- ¿Qué deberá hacer?
- ¿Cómo lo deberá hacer?
- ¿Cuál es la justificación para que se haga de la manera señalada?
- ¿Cuál es la secuencia y ocurrencia de los datos?
- La definición del proceso.
- Los archivos y bases de datos utilizados.
- Las salidas y reportes.

Una vez que se han analizado estas partes, se deberá estudiar la participación que tuvo el usuario en la identificación del nuevo sistema, la participación de auditoria interna en el diseño de los controles y la determinación de los procedimientos de operación y decisión. Al tener el análisis del diseño lógico del sistema se debe compararlo con lo que realmente está obteniendo: como en el caso de la administración, en la cual se debe evaluar lo planeado, cómo fue planeado y lo que, realmente se está obteniendo (lo real).

III.5.- Programas de Desarrollo.

Los programas de desarrollo incluyen *"software"* que sólo puede ser usado por el personal que ha tenido entrenamiento y experiencia, (Gratton, 1998); este *"software"* incluye:

A). Lenguajes de Programación:

- Lenguaje de máquina.
- Ensambladores.
- De tercera generación.
- De cuarta generación:
  - ✓ 4GLS.
  - ✓ Query languages.
  - ✓ Generadores de reportes.
  - ✓ Lenguajes naturales.
  - ✓ Generaciones de aplicaciones.

B). CASE (*Computer Aided Software Engineering*).

C). Programación Orientada a Objetos.

Al utilizar un determinado *"software"* se debe evaluar lo siguiente:

- Interfases de usuario gráfico para poder diseñar pantallas y reportes agradables y visuales.
- Enlace de objetos en los Sistemas de Información. Esto permite unir determinados objetos dentro de un documento; por ejemplo, unir un procesador de palabra con una hoja de cálculo, o bien unir información de un programa o sistema a otro programa o sistema.
- Capacidad de trabajar en multiplataformas.
- Capacidad de trabajar en redes.
- Licencias. Verificar el tipo de licencia que se puede contratar (individual, múltiple, corporativa, etcétera).
- Transportable.
- Compatible con otro *"software"*.
- Compatible con periféricos.
- Fácil de usar.
- Grado de mejora(s).
- Capacidad de utilización en red.
- De fácil instalación.
- Demanda en arquitectura de sistemas *"Hardware"*.
- Requerimientos de memoria.
- Costo.
- Seguridad y confidencialidad.

III.6.- Bases de Datos.

El banco de datos es el conjunto de datos que guardan entre sí una coherencia temática independiente del medio de almacenamiento. La cantidad de información que contiene un banco de datos suele ser muy grande, del orden de millones de datos. Se considera que una Base de Datos es la organización sistemática de archivos de datos para facilitar su acceso, recuperación y actualización, los cuales están relacionados unos con otros y son tratados como una entidad. Puede decirse que una Base de Datos es un banco de datos organizado como un tipo estructurado de datos. El DBMS (Data Base Management System) es un conjunto de programas que permite manejar cómodamente una base de datos, o sea: "El conjunto de facilidades y herramientas de actualización y recuperación de información de una Base de Datos", (Vaquero y Jopnes, 2002).

En las bases de datos se debe evaluar:

- La independencia de los datos. Muchos de los programas elaborados internamente eran independientes de los archivos creados por ellos mismos, o sea que carecían de independencia. La falta de independencia significa que cada vez que un archivo es cambiado, todo programa que accede a ese archivo debe ser cambiado.
- Redundancia de los datos. Se deben evitar las redundancias en las bases de datos.
- Consistencia de los datos. El problema de redundancia en los datos no sólo provoca que se ocupe demasiado espacio en los discos, sino que también puede causar el problema de inconsistencia en los datos, ya que se puede cambiar en un archivo pero omitirse en algún otro de los archivos.

Un Sistema de Base(s) de Datos es un conjunto de programas que:

- Almacena los datos en forma uniforme y de manera consistente.
- Organiza los datos en archivos en forma uniforme y consistente.
- Permite el acceso a la información en forma uniforme y consistente.
- Elimina la redundancia innecesaria en los archivos.

Los componentes a evaluar dentro de una Base de Datos son:

- Diccionario / directorio de datos.
- Lenguajes de datos (lenguajes de descripción de datos: DDL, lenguajes de manipulación de datos: DML).
- Monitoreo de teleproceso
- Herramientas de desarrollo de aplicaciones.
- *"Software"* de seguridad.
- Sistemas de almacenamiento, respaldo y recuperación.
- Reporteadores.
- *Query languages (Structured Query Language: SQL; Natural Language Queries, query by example: QBE).*
- Bases de Datos multiplataformas.
- *Web Server Software (World Wide Web: www).*

III.7.- El Administrador de Bases de Datos.

El desarrollo de las bases de datos ha creado la necesidad dentro de la Organización de contar con un organismo encargado de administrar las bases de datos cuyas funciones son las de planear, diseñar, organizar, operar, entrenar, así como dar soporte a los usuarios, seguridad y mantenimiento.

Dentro de las funciones de este organismo, están las de tener relaciones con la alta administración, los analistas de sistemas, los programadores de aplicaciones, los usuarios y los programadores de sistemas. Los modelos de bases de datos pueden ser:

- Jerárquicos.
- De redes.
- Relacionales.
- Orientados a objetos.

Entre las ventajas del sistema de bases de datos se encuentran:

- ✓ Compartir datos.
- ✓ Reducción de redundancia de datos.
- ✓ Mejora de la consistencia de los datos.
- ✓ Independencia de datos.
- ✓ Incrementa la productividad del programador de aplicaciones y de usuarios.
- ✓ Mejora el control y la administración de los datos.
- ✓ Incrementa el énfasis de los datos como un recurso. Aumenta la importancia de la información como parte fundamental de la administración.

III.7.1.- Problemas de los Sistemas de Administración de Bases de Datos.

Cuando varios usuarios utilizan una Base de Datos, pueden existir problemas si no fue diseñada para usuarios múltiples. Uno de estos problemas surge cuando no existe un control sobre la actualización inmediata. Esto significa que dos o más usuarios pueden estar elaborando cambios al mismo archivo en el mismo momento, y no existe control sobre la actualización inmediata de los archivos. Este tipo de problemas existe principalmente en las Bases de Datos de ordenadores personales, ya que los grandes sistemas tienen control sobre las actualizaciones inmediatas. También pueden existir problemas en el uso de recursos excesivos de cómputo, lo cual se agrava si no se tiene un mantenimiento constante sobre las bases de datos, (Derrien, 1995).

Problemas de seguridad. Las bases de datos deben tener suficiente control para que se asegure que sólo personal autorizado pueda acceder datos, y se debe definir el tipo de usuario que pueda adicionar, dar de baja, actualizar o acceder datos dependiendo de su llave de entrada, así como el usuario propietario de la base de datos.

III.8.- Comunicación.

Se debe evaluar el modo de comunicación y el código empleado. Los diferentes modos de comunicación varían dependiendo del tipo de información que se transmite y el costo del medio empleado.

El medio de comunicación es también un factor importante a evaluar, y éste dependerá de la velocidad y capacidad de transmisión, lo cual está directamente relacionado con el costo (cables trenzados, cable coaxial, fibra óptica, microondas, ondas de radio, infrarrojas, etcétera), Tanenbaum (1997). Los componentes más comunes dentro de un sistema de comunicaciones son:

- Servidor y huésped.
- Terminal o Estación de Trabajo.
- Convertidores de Protocolo.
- Módem.
- Equipo de conexión de terminales.
- Modo de Comunicación.
- Medio de Comunicación.
- Topología de la(s) Red(es):
    - De punto a punto, o estrella y topología jerárquica.
    - *"Multidrop"* o Bus y *"Token Ring"*.
    - *"Mesh"*.
    - Sin cables (*wireless*).
        - Tipo de Redes:
        - Local.
        - *Wide Area Networks (WAN)*.
        - Enterprise.
        - Internacional.

En general, las redes pueden ser caras y pueden crear complicaciones en el sistema de información, pero pueden ser justificables por alguna o varias de las razones siguientes:

- Compartir periféricos.
- Compartir archivos.
- Compartir aplicaciones.
- Reducir costos de adquisición, instalación y mantenimiento de *"software"*.
- Conexión con otras redes.
- Captura de datos en lugares que son de información.
- Aumentar la productividad.

- Permitir la expansión.
- Disminuir el tiempo de comunicación.
- Aumentar el control.
- Seguridad.

Los puntos a revisar en las redes son:

- Confiabilidad de las redes. Un sistema con redes que estén constantemente *"caídas"*, o que no sea confiable, provoca muchos problemas a la Organización. Y cuestiona su funcionamiento.
- Tiempo de respuesta. Una red que sea lenta en sus operaciones, provoca que los usuarios la eviten o no la utilicen. Entre los problemas que puede ocasionar esa lentitud están:
  - La distancia que tiene que recorrer y la forma en que se transmite.
  - La cantidad de tráfico en la red.
  - La capacidad de los canales de comunicación.
  - Factores externos a la red, como puede ser la estructura de las bases de datos.
- Costo de la red.
- Compatibilidad con otras redes.
- Seguridad en las redes.

Los puntos a evaluar en el diseño lógico del sistema son:

- Entradas.
- Salidas.
- Procesos.
- Especificaciones de datos.
- Especificaciones de proceso.
- Métodos de acceso.
- Operaciones.
- Manipulaciones de datos (antes y después del proceso electrónico de datos).
- Proceso lógico (necesario para producir informes).
- Identificación de archivos, tamaño de los campos y registros.
- Proceso en línea o lote y su justificación.
- Frecuencia y volúmenes de operación.
- Sistemas de seguridad.
- Sistemas de control.
- Responsables (tipos de usuario, identificando los usuarios propietarios de la información).
- Nuevos usuarios.
- *"Software"* necesario.
- Bases de Datos requeridas.
- En caso de redes, determinar su tipo y características.

III.9.- Informes.

Cuando se analiza un sistema de informática es muy común pensar exclusivamente en la parte relacionada con la Informática, y se olvida de que un sistema comprende desde el momento en que se genera un dato, así como su procesamiento, realimentación y salida, (Tanenbaum, 1997). Es muy común que solamente se evalúe el procesamiento de la información y su almacenamiento dejando fuera la evaluación de aquello que es el inicio del sistema, el seguimiento administrativo y la obtención de los reportes y salidas de información. Lo que se debe determinar en el sistema es:

- En el procedimiento:
  - ¿Quién hace la función, cuándo y cómo?
  - ¿Qué formas se utilizan en el sistema?
  - ¿Son necesarias, se usan, están duplicadas?
  - ¿El número de copias es el adecuado?
  - ¿Existen puntos de control o faltan?
- En la gráfica de flujo de información:
  - ¿Es fácil de usar?
  - ¿Es lógica?
  - ¿Se encontraron lagunas?
  - ¿Hay faltas de control?
- En las formas de diseño:
  - ¿Cómo está usada la forma en el sistema?
  - ¿Qué tan bien se ajusta la forma al procedimiento?
  - ¿Cuál es el propósito, por qué se usa?
  - ¿Se usa y se necesita?
  - ¿El número de copias es el adecuado?
  - ¿Quién lo usa?

Entre los elementos a revisar en el diseño de formas están:

Numeración. ¿Está numerada la forma?, ¿Es necesaria la numeración?, ¿Está situada en un solo lugar fácil de encontrar?, ¿Cómo de controlan las hojas numeradas y su utilización.

Espacio. Si la forma va ser mecanografiada, ¿hay suficiente espacio para escribir a máquina rápidamente, con exactitud y eficiencia? Si la forma se llenará a mano, ¿hay espacio adecuado y suficiente para que se escriba en forma legible?

Tabulación. Si la forma va ser mecanografiada, ¿permite su tabulación llenarla uniformemente?, ¿Es la tabulación mínima posible? Una excesiva tabulación disminuye la velocidad y eficiencia para llenarla. Además, le da una apariencia desigual y confusa.

Zonas. ¿Están juntos los datos relacionados entre sí? Si los datos similares están agrupados por zonas, todas las personas que usan la forma ahorran tiempo. La información similar es reunida por zonas para hacer más fácil su referencia, se mecanografía más eficientemente y se revisa con más rapidez. Posteriormente, se debe verificar que las zonas de las formas que sean utilizadas para captura estén situadas de manera congruente con el diseño de las pantallas de captura.

Rayado. ¿Da la forma una apariencia desordenada y difícil de entender por el uso confuso y excesivo de líneas delgadas, gruesas o de doble raya?

Instrucciones. ¿Se le dice al usuario cómo debe llenar la forma? Formas autoinstructivas o que suministran la información de cómo llenarlas permiten que el personal nuevo y los otros trabajen con supervisión y errores mínimos. De no ser así, existe un manual de llenado de formas, el cual se debe revisar para ver si las instrucciones son claras, si son congruentes con la forma y si son excesivas, ya que un diseño excesivo de instrucciones puede provocar confusión y hacer que éstas sean poco claras.

Firmas. ¿Existe suficiente espacio para una firma legible?, ¿Está el espacio debidamente identificado respecto a la firma que se solicita?, ¿La firma se utiliza como un mero trámite o realmente controla la persona que firma lo que se está firmando?

Nombres. ¿Se usan los nombres de los puestos en lugar del nombre del individuo en la forma? No es conveniente imprimir nombres de personas debido a la rotación de personal.

Encabezados ambigüos. ¿Se indica con exactitud qué fechas, qué números o qué firmas se requieren? Se debe evitar encabezados dudosos o ambigüos.

Rótulos. ¿Son demasiado llamativos?, ¿Son demasiado discretos?, ¿Existe un adecuado contraste entre los rótulos y los textos respecto su tamaño, color y ubicación, para que los datos solicitados sean identificados fácilmente?

Ubicación de los rótulos. ¿Están los rótulos o encabezados debajo de la línea en donde se debe mecanografiar? Esto causa pérdida de tiempo, porque la mecanógrafa tiene que mover el carro para ver el rótulo y acomodarlo nuevamente para escribir la forma deseada.

Casilleros. ¿Se usan pequeños espacios enmarcados ( ) para con una sola indicación reducir escritos largos o repetitivos?, ¿Los espacios son suficientes o excesivos?

Tipo de papel. ¿Son el peso y calidad del papel apropiados para esa forma? Usar papel más pesado y de mejor calidad para aquellas formas que requieren un manejo excesivo. Usar papel de menor peso con formas que se usen poco, para reducir costo y espacio en los archivos.

Tamaños estándar. ¿Tiene la forma un tamaño estándar se ajusta a sobres y archivos estándar. Además, reduce existencias de papel, manejo, tiempo y costo de impresión. Se debe considerar que el costo del papel que no es de tamaño estándar es considerablemente mayor que el de tamaño estándar.

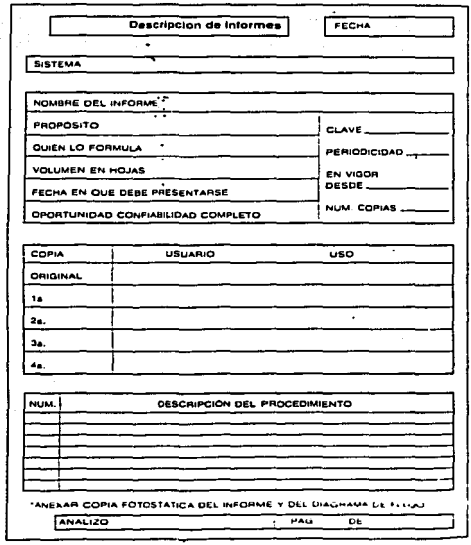
Color. ¿Permite el contraste del color del papel una lectura eficiente? Las formas en colores, como el anaranjado, el verde, el azul, el gris, etcétera; en tonos oscuros, son difíciles de leer porque no ofrecen suficiente contraste entre la impresión (negro) y el papel. Ciertos colores brillantes cansan la vista. Se debe tener cuidado tanto en el color del papel como en el color de la tinta. Las copias deben estar identificadas de acuerdo con el color. Como ejemplo de análisis de formas véase las Figuras III.3, III.4 y III.5; para la descripción de formas véase las Figuras III.6 y III.7.

III.10.- Análisis de Informes.

Una vez que se han estudiado los formatos de entrada se debe analizar los informes para posteriormente evaluarlos con la información proporcionada por la encuesta a los usuarios. Como ejemplo de la descripción de los informes véase la Figura III.1, y para el análisis de los informes véase la Figura III.2. Después de describir el contenido de los informes se debe tener el análisis de datos e información.

III.11.- Ruido, Redundancia y Entropía.

En la Auditoría de Sistemas hay que estudiar la redundancia, el ruido y la entropía que tiene cada uno de los sistemas. En primer lugar, se debe considerar como comunicación: *"La transferencia de información del emisor al receptor de manera que éste la comprenda"*. (Koontz y O' Donnel, 2000).



Descripcion de Informes

FECHA

SISTEMA

NOMBRE DEL INFORME

PROPOSITO

QUIEN LO FORMULA

VOLUMEN EN HOJAS

FECHA EN QUE DEBE PRESENTARSE

OPORTUNIDAD CONFIABILIDAD COMPLETO

CLAVE

PERIODICIDAD

EN VIGOR DESDE

NUM COPIAS

COPIA	USUARIO	USO
ORIGINAL		
1a.		
2a.		
3a.		
4a.		

NUM.	DESCRIPCION DEL PROCEDIMIENTO

*ANEXAR COPIA FOTOSTATICA DEL INFORME Y DEL DIAGRAMA DE FLUJO

ANALIZO PAG DE

Figura III.1.- Descripción de Informes.

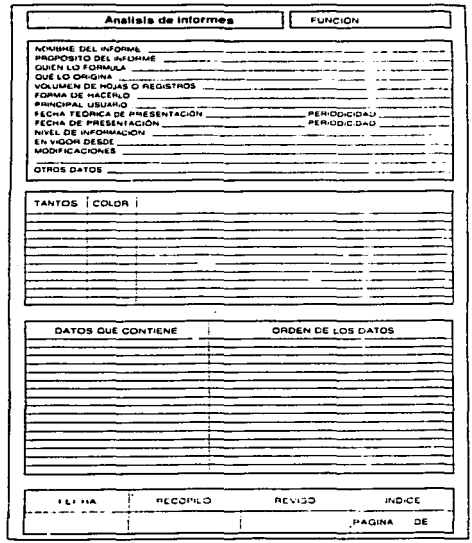


Figura III.2.- Análisis de informes.

Evaluacion de formas

NOMBRE DE LA FORMA	FRECUENCIA DE USO
ELABORADO POR	NUM DE FORMA / NUM DE COPIAS
USUARIOS	CANT IMPRESA / CANT INV
	PERIODO ESTIMADO DE USO
OBSERVACIONES	

FACTORES A EVALUAR

INFORMACION EMPRESA			IMAGEN		
TERMINOLOGIA ESTANDAR	SI	NO	PROFESIONAL Y CORRECTA	SI	NO
EXISTE MANUAL DE OPERACION	SI	NO	CALIDAD APROPIADA DE PAPEL	SI	NO
AUTODESCRIPTIVA	SI	NO	BUENA CALIDAD DE IMPRESION	SI	NO
FUENTE DE INFORMACION DEBIDAMENTE IDENTIFICADA	SI	NO	COSTO		
REQUIERE OTROS DATOS DE REFERENCIA	SI	NO	MAXIMO APROVECHAMIENTO DE PAPEL	SI	NO
TIENE SUFICIENTES ESPACIOS	SI	NO	MAXIMO APROVECHAMIENTO DE IMPRESION	SI	NO
DATOS QUE CONTIENE			CUMPLE CON LAS NECESIDADES	SI	NO
NECESITA DATOS ADICIONALES	SI	NO	DUPLICA DATOS DE OTRAS FORMAS	SI	NO
TIENE DATOS INNECESARIOS	SI	NO			

EN CASO DE HABER CONTESTADO "NO" A ALGUNA PREGUNTA, ANOTE LAS OBSERVACIONES

Figura III.3.- Evaluación de Formas.

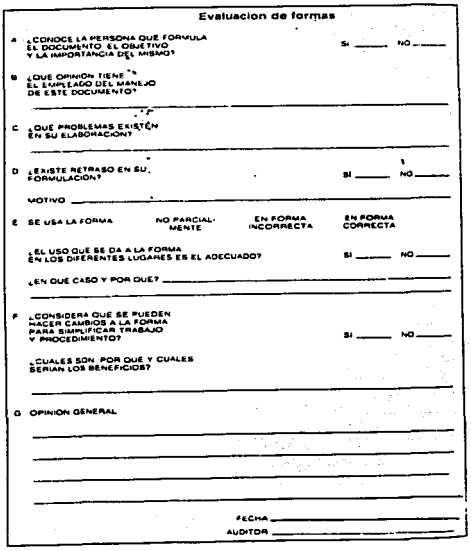
Evaluacion de formas FECHA ____ ____

UTILIZACION			PREPARACION		
ENCABEZADOS EN ORDEN CRONOLOGICO	SI	NO	RENGLONES DE DATOS EN ORDEN CRONOLOGICO SIGUIENDO	SI	NO
FORMATOS ESTANDAR	SI	NO	DATOS CONSTANTES PREIMPRESOS	SI	NO
DESCRIBE CLARAMENTE EL USUARIO	SI	NO	ESPACIOS SUFICIENTES SEGUN MANERA DE PREPARACION	SI	NO
COPIAS FACIL DE IDENTIFICAR	SI	NO	COPIAS FACIL DE SEPARARSE	SI	NO
COPIAS CLARAS PARA UN BUEN REGISTRO	SI	NO	TABULACION UNIFORME	SI	NO
SUFICIENTE CALIDAD DEL PAPEL PARA LA VIDA DE LA FORMA	SI	NO	ENCABEZADOS ARRIBA DE LAS AREAS PARA LLENAR	SI	NO
FACIL DE MANEJAR Y ARCHIVAR	SI	NO	UTILIZA ESPACIOS ENMARCADOS	SI	NO
FACIL DE IMPRIMIR O REPRODUCIR	SI	NO	MEDIDA ESTANDAR DE PAPEL	SI	NO
TITULOS Y ENCABEZADOS BIEN BALANCEADOS	SI	NO	CALIDAD DE PAPEL APROPIADO	SI	NO
			ES CONGRUENTE CON LAS PANTALLAS DE CAPTURA	SI	NO
CONTROL					
NUMERO DE CLAVE	SI	NO	REQUIERE NUMERO DE CONTROL SECUENCIAL	SI	NO
REQUIERE AUTORIZACION PARA REIMPRIMIRSE	SI	NO			

EN CASO DE HABER CONTESTADO "NO" A ALGUNA PREGUNTA, ANOTE LAS OBSERVACIONES

ANALIZADO POR

Figura III.4.- Evaluación de Formas.



Evaluacion de formas

A ¿CONOCE LA PERSONA QUE FORMULA EL DOCUMENTO EL OBJETIVO Y LA IMPORTANCIA DEL MISMO? SI _____ NO _____

B ¿QUE OPINIÓN TIENE EL EMPLEADO DEL MANEJO DE ESTE DOCUMENTO?

_____

C ¿QUE PROBLEMAS EXISTEN EN SU ELABORACION?

_____

D ¿EXISTE RETRASO EN SU FORMULACION? SI _____ NO _____

MOTIVO _____

E SE USA LA FORMA NO PARCIALMENTE EN FORMA INCORRECTA EN FORMA CORRECTA

¿EL USO QUE SE DA A LA FORMA EN LOS DIFERENTES LUGARES ES EL ADECUADO? SI _____ NO _____

¿EN QUE CASO Y POR QUE? _____

_____

F ¿CONSIDERA QUE SE PUEDEN HACER CAMBIOS A LA FORMA PARA SIMPLIFICAR TRABAJO Y PROCEDIMIENTO? SI _____ NO _____

¿CUALES SON, POR QUE Y CUALES SERIAN LOS BENEFICIOS?

_____

G OPINIÓN GENERAL

_____

_____

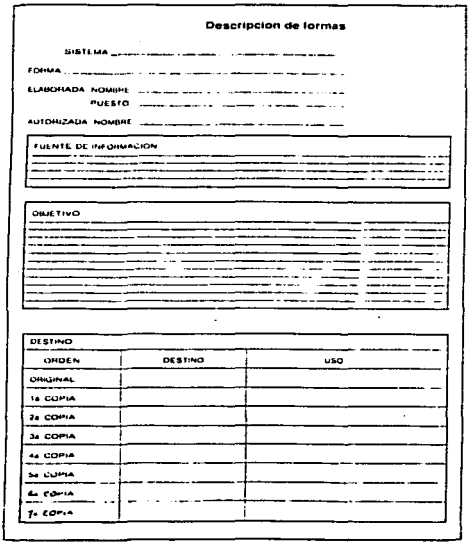
_____

_____

FECHA _____

AUDITOR _____

Figura III.5.- Evaluación de Formas.



Descripcion de formas

SISTEMA

FORMA

ELABORADA NOMBRE

PUESTO

AUTORIZADA NOMBRE

FUENTE DE INFORMACION

OBJETIVO

DESTINO

ORDEN	DESTINO	USO
ORIGINAL		
1a COPIA		
2a COPIA		
3a COPIA		
4a COPIA		
5a COPIA		
6a COPIA		
7a COPIA		

Figura III.6.- Descripción de Formas.

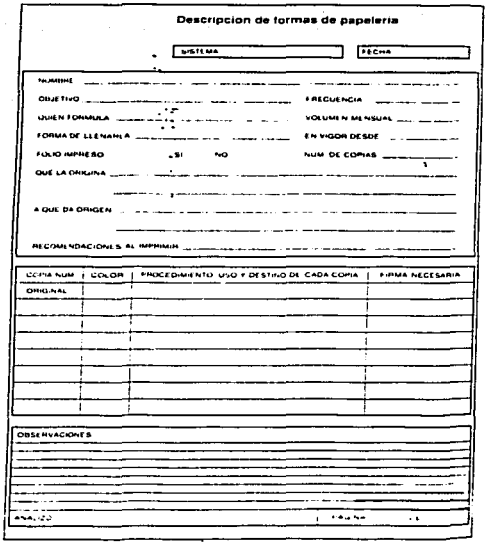


Figura III.7.- Descripción de Formas de Papelería.

El ruido es todo aquello que interfiere en una adecuada comunicación; no solamente los sonidos sino aquello que impida la adecuada comunicación: *"Cualquier cosa (sea en el emisor, en la transmisión o en el receptor) que obstaculiza la comunicación"*. (Koontz y O' Donnel, 2000).

En el caso de un sistema computarizado, el error en una captura, una pantalla de la terminal demasiado llena de información y poco entendible o un reporte inadecuado se deben considerar como ruido en el sistema, ya que impiden una buena comunicación de la información. En el caso de los sistemas se debe evaluar lo que se conoce como *"sistema amigable"*, lo cual significa:

- Que tenga las ayudas necesarias para el caso de alguna duda *(help)*.
- Que contenga os catálogos necesarios para el caso de referencias.
- Que tenga las ligas automáticas con otros sistemas para obtener información o para consulta (conexiones automáticas a otras bases de datos o redes).
- Que la información sea solicitada en forma secuencial y lógica.
- Que sea de fácil lectura y, en su caso, escritura.
- Que sea rápido, ágil, y que contenga una limpieza que permita una fácil visualización.

La redundancia es toda aquella duplicidad que tiene el sistema con la finalidad de que, en caso de que exista ruido, permita que la información llegue al receptor en forma adecuada.

La redundancia puede ser conveniente en el caso de que haya que cerciorarse de que la información se recibe correctamente. Esto estará en función de lo delicada que sea la información y del riesgo que se corre en caso de una pérdida total o parcial de la misma.

La redundancia es una forma de control que permite que, aunque exista ruido, la comunicación pueda llevarse a cabo en forma eficiente; deberá haber mayor redundancia entre más arriesgada, costosa o peligrosa sea la pérdida de información, aunque, a la vez se debe estar conciente de que el exceso de redundancia puede provocar ruido.

En la auditoria se debe considerar que todo el sistema ha de ofrecer un número adecuado de redundancia, según su nivel de importancia, de modo que permita una buena comunicación, aún en el caso de que exista ruido, pero sin ser la redundancia de tal magnitud que a su vez provoque ruido.

También se debe considerar que con un mayor control y redundancia se incrementa también el costo de los sistemas. Hay que tener un adecuado nivel de control y redundancia, que no sea de tal magnitud que provoque ruido o bien que no sea demasiado costoso en relación con el nivel de seguridad que requiere el sistema.

III.11.1.- Entropía.

El diccionario la define como: *"Cantidad de Energía que por su degradación no puede aprovecharse"*. (Diccionario Sopena Ilustrado, 2002).

La Entropia en un Sistema; por ejemplo de un motor, es el calor que genera, el cual es energía que por sus características no puede aprovecharse. En el caso del sistema llamado motor se utiliza esta Entropía. En un sistema computarizado se debe procurar reducir al máximo esta entropía, y una de las formas de reducirla es interconectar sistemas, de tal manera que esa cantidad de energía no usada en un sistema pueda ser utilizada en otro sistema.

III.12.- Evaluación del Desarrollo del Sistema.

En esta etapa del sistema se deberá auditar los programas, su diseño, el lenguaje utilizado, la interconexión entre los programas y las características de la arquitectura de sistemas empleado (total o parcial) para el desarrollo del sistema.

Al evaluar un sistema de información se tendrá presente que todo sistema debe proporcionar información para planear, organizar y controlar de manera eficaz y oportuna, así como para reducir la duplicidad de datos y de reportes, y obtener una mayor seguridad en la forma más económica posible. De este modo se contará con los mejores elementos para una adecuada toma de decisiones.

III.13.- Sistemas Distribuidos, Internet, Comunicación entre Oficinas.

Los sistemas distribuidos se pueden definir como el sistema en el cual los ordenadores y los datos están en más de un lugar (*site*), así como los programas de aplicación, (echenique, 2001). Ejemplos de esto son las redes WAN, PBX, LAN, Internet. Las razones para implementar un sistema distribuido son:

- Mejora del tiempo de respuesta.
- Reducción de costos.
- Mejora de exactitud en la actualización.
- Reducción del costo del ordenador principal (*mainframe*) y la dependencia a un solo ordenador.

- Puede tenerse un crecimiento planeado. En lugar de grandes equipos que dificultan su administración, organización, y que requieren de espacios muy amplios, se tienen equipos descentralizados que son más fáciles de administrar y de controlar su crecimiento.
- Incremento de confianza, ya que si falla el equipo principal no significa que falle todo el sistema.
- Compartir recursos.
- Aumenta la satisfacción de los usuarios, ya que los ordenadores y el desarrollo pueden estar cerca del usuario.
- En bases de datos se puede usar el concepto Cliente / Servidor y *Structured Query Language* (SQL).

Los puntos que se deben considerar al evaluar un sistema distribuido son:

- Falta de personal calificado en todos los puntos del sistema.
- Estandarización
- Documentación.
- Pérdida de datos.
- Seguridad.
- Consistencia de los datos.
- Mantenimiento del sistema.

Al tener un proceso distribuido es preciso considerar la seguridad del movimiento de la información entre nodos. El proceso de planeación de sistemas debe definir la red óptima de comunicaciones, recordando que el plan de aplicaciones proporciona información de la ubicación planeada de las terminales, los tipos de mensajes requeridos, el tráfico esperado en las líneas de comunicación y otros factores que afectan el diseño. Es importante considerar las variables que afectan a un sistema; ubicación en los niveles de la Organización, tamaño y recursos que utiliza. Las características que deben evaluarse en los sistema son:

- Dinámicos (susceptibles de modificarse).
- Transportables (que puedan ser usados en diferentes máquinas y en diferentes plataformas).
- Estructurados (las interacciones de sus componentes o subsistemas deben actuar como un todo).
- Integrados (un solo objetivo). En él habrá sistemas que puedan ser interrelacionados y no programas aislados.
- Accesibles (que estén disponibles).
- Necesarios (que se pruebe su utilización).
- Comprensibles (que contengan todos los atributos).
- Oportunos (que esté la información en el momento que se requiere).
- Funcionales (que proporcionen la información adecuada a cada nivel).
- Estándar (que la información tenga la misma interpretación en los distintos niveles).
- Modulares (facilidad para ser expandidos o reducidos).

- Seguros (que sólo las personas autorizadas tengan acceso).
- Únicos (que no dupliquen información).

En relación con otros sistemas deben de estar interconectados de tal forma que permitan un sistema integral, y no una serie de programas o sistemas aislados. Se deben de tener sistemas que tengan la necesaria redundancia, pero que ésta no sea tan grande que provoque que el sistema sea lento o ineficiente.

III.14.- Control de Proyectos.

Debido a las características propias del análisis y de la programación es muy frecuente que la implantación de los sistemas se retrase, y llegue a suceder que una persona trabaje varios años en un sistema o bien que se presenten irregularidades en las que los programadores realizan actividades ajenas a la Dirección de Informática. Para poder controlar el avance de los sistemas, ya que se trata de una actividad intelectual de difícil evaluación, se recomienda que se utilice la técnica de administración por proyectos para su adecuado control.

¿Qué significa que un sistema sea liberado en el plazo establecido y dentro del presupuesto? Pues sencillamente que el grado de control en el desarrollo del mismo es el adecuado o tal vez el óptimo. Pero esto no se consigue gratuitamente o porque la experiencia o calidad del personal de desarrollo sea alta, sino porque existe un grado de control durante su desarrollo que permite obtener esta cualidad. Cabe preguntar aquí: ¿quién es realmente el elemento adecuado para proporcionar este grado de control?

Para poder tener una buena administración por proyectos se requiere que el analista o el programador y su jefe inmediato elaboren un plan de trabajo en el cual se especifiquen actividades, metas, personal participante y tiempos. Este plan debe ser revisado periódicamente (semanal, mensual o bimestralmente) para evaluar el avance respecto a lo programado.

La estructura estándar de la planeación de proyectos deberá incluir la facilidad de asignar fechas predefinidas de terminación de cada tarea. Entre estas fechas debe estar el calendario de reuniones de revisión, las cuales tendrán diferentes niveles de detalle. Son necesarias las reuniones a nivel técnico con la participación del personal especializado de la Dirección de Informática, para definir la factibilidad de la solución y los resultados planeados. Son muy importantes las reuniones con los usuarios finales, para verificar la validez de los resultados esperados. La evaluación de proyectos y su control puede realizarse de acuerdo con diferentes autores.

Incluir el plazo estimado de acuerdo con los proyectos que se tienen para que el Departamento de Informática satisfaga las necesidades de la dependencia, según la situación actual. Como ejemplo de formato de control de proyectos véase la Figura III.8; del calendario de actividades véase las Figuras III.9 y III.10; del reporte de los responsables del sistema, véase la Figura III.11; del control de programadores véase la Figura III.12; de planeación de la programación véase las Figuras III.13 y III.14; de los informes de avance de la programación véase la Figura III.15; de control de avance de programación véase Figuras III.16 y III.17. Se deberán revisar tanto los proyectos terminados como los que se encuentran en proceso, para verificar si se ha cumplido con el plan de trabajo o si cumple con su función de medio de control.

III.15.- Control de Diseño de Sistemas y Programación.

El objetivo de esto es asegurarse de que el sistema funcione conforme a las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación. Las revisiones se efectúan en forma paralela, desde el análisis hasta la programación, y sus objetivos son los siguientes:

Etapa de análisis y definición del problema.- Identificar con claridad cuál es el objetivo del sistema, eliminando inexactitud, ambigüedades y omisiones en las especificaciones.

Etapa de estudio de factibilidad.- Elaborar el costo / beneficio del sistema, desarrollando el modelo lógico, hasta llegar a la decisión de elaborarlo o rechazarlo, incluyendo el estudio de factibilidad técnico y las recomendaciones.

Etapa de diseño.- Desarrollar los objetivos del sistema; desarrollar el modelo lógico; evaluar diferentes opciones de diseño, y descubrir errores, debilidades, omisiones, antes de iniciarse la codificación. Esta actividad es muy importante ya que el costo de corregir errores es directamente proporcionar al momento en que se detectan si se descubren en el momento de programación será más alto el costo que si se detectan en la etapa de análisis. El análisis deberá proporcionar la descripción del funcionamiento del sistema funcional desde el punto de vista del usuario, indicando todas las interacciones del sistema, la descripción lógica de cada dato, las estructuras que éstos toman, el flujo de información que tiene lugar en el sistema. Así mismo, se indicará lo que el sistema tomará como entradas, los procesos que serán realizados, las salidas que deberá proporcionar, los controles que se efectuarán para cada variable y los procedimientos.

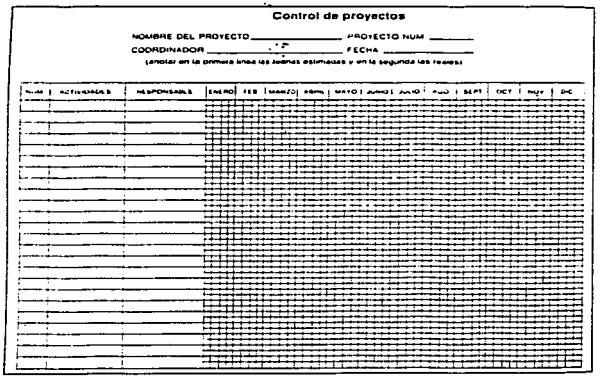


Figura III.8.- Control de Proyectos.

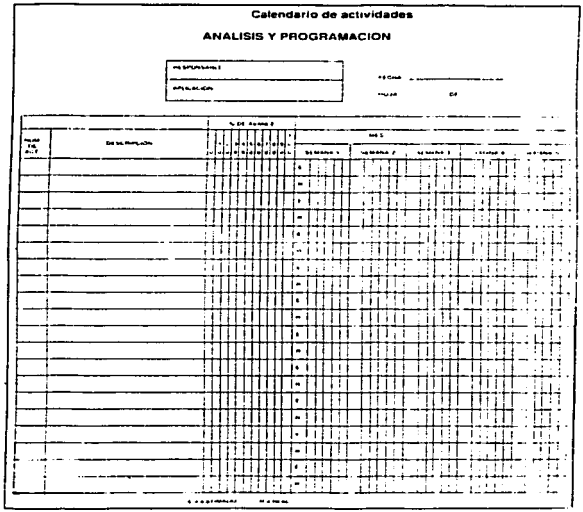
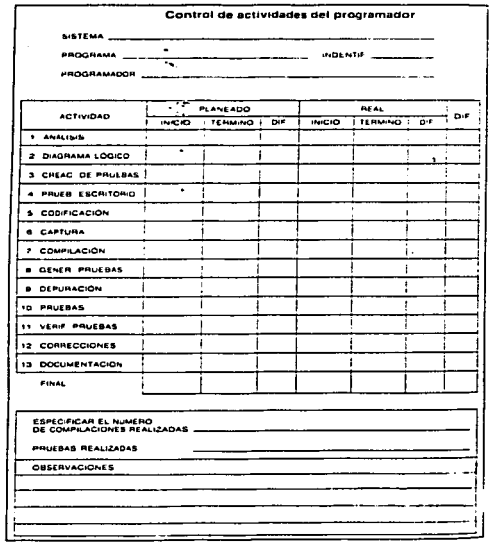


Figura III.9.- Calendario de Actividades.



Control de actividades del programador

SISTEMA _____

PROGRAMA _____ IDENTIF _____

PROGRAMADOR _____

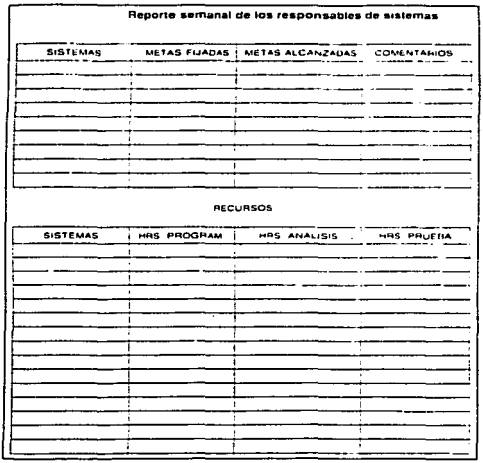
ACTIVIDAD	PLANEADO			REAL			DIF
	INICIO	TERMINO	DIF	INICIO	TERMINO	DIF	
1 ANALISIS							
2 DIAGRAMA LOGICO							
3 CREAC DE PRUEBAS							
4 PRUEB ESCRITORIO							
5 CODIFICACION							
6 CAPTURA							
7 COMPILACION							
8 GENER PRUEBAS							
9 DEPURACION							
10 PRUEBAS							
11 VERIF PRUEBAS							
12 CORRECCIONES							
13 DOCUMENTACION							
FINAL							

ESPECIFICAR EL NUMERO DE COMPILACIONES REALIZADAS _____

PRUEBAS REALIZADAS _____

OBSERVACIONES

Figura III.10.- Control de Actividades del Programador.



Reporte semanal de los responsables de sistemas

SISTEMAS	METAS FIJADAS	METAS ALCANZADAS	COMENTARIOS

RECURSOS

SISTEMAS	HRS PROGRAM	HRS ANALISIS	HRS PRUEBA

Figura III.11.- Reporte Semanal de los Responsables de Sistemas.

Control de programadores													
PROGRAMA A REALIZAR	NOMBRE DEL RESPONSABLE	DIAGRAMA		CODIFICACION		CAPTURA		PRUEBAS		IMPLANTACION		OPERACION	
		FECHA INIC	FECHA FINAL	FECHA INIC	FECHA FINAL	FECHA INIC	FECHA FINAL	FECHA INIC	FECHA FINAL	FECHA INIC	FECHA FINAL	FECHA INIC	FECHA FINAL

Figura III.12.- Control de Programadores.

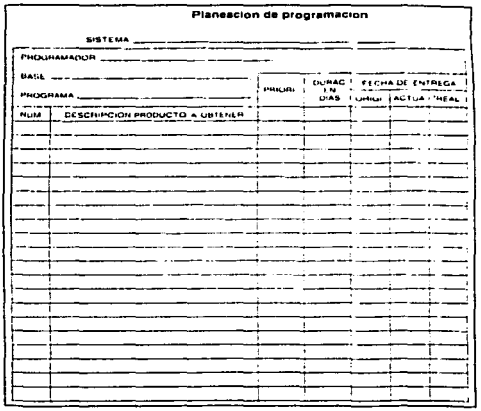
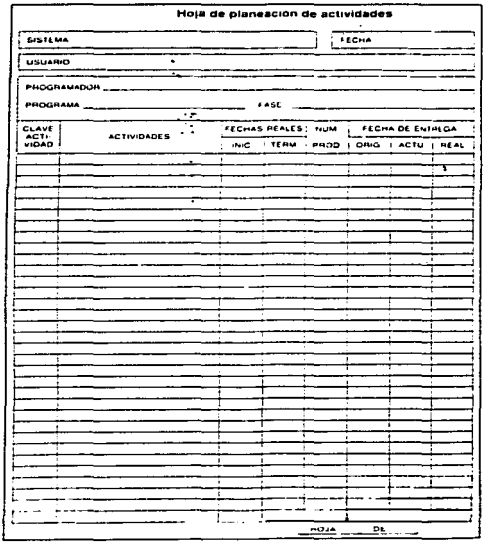


Figura III.13.- Planeación de Programación.



Hoja de planeacion de actividades

SISTEMA | FECHA

USUARIO

PROGRAMADOR

PROGRAMA | FASE

CLAVE ACTIVIDAD	ACTIVIDADES	FECHAS REALES		NUM	FECHA DE ENTREGA		
		INIC	TERM	PROD	ORIG	ACTU	REAL

HOJA DE

Figura III.14.- Hoja de Planeación de Actividades.

Informe de avance de programacion

FECHA HOJA DE

SISTEMA

RESPONSABLE

PROGRAMAS TERMINADOS A LA FECHA		
NUM FASE	NUM PROG	FECHA ENTREGA

PROG CON DESVIACION O CANCELACION		
NUM FASE	NUM PROG	NUEVA FECHA

NUEVOS PROGRAMAS A INCLUIR EN EL PLAN				
NUM FASE	NUM PROG	DESCRIPCION	DURACION DIAS	FECHA ENTREGA DEL PROGRAMA

Figura III.15.- Informe de Avance de Programación.

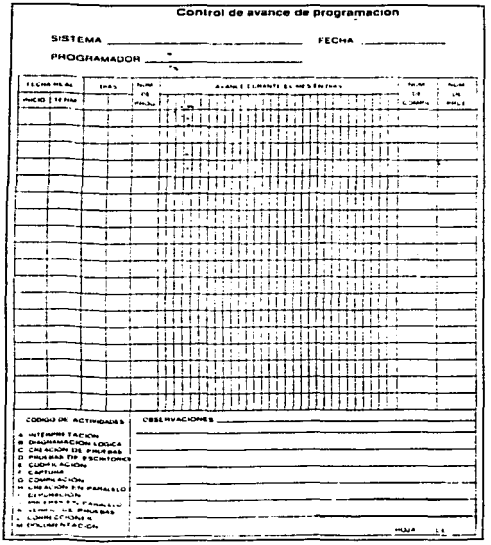
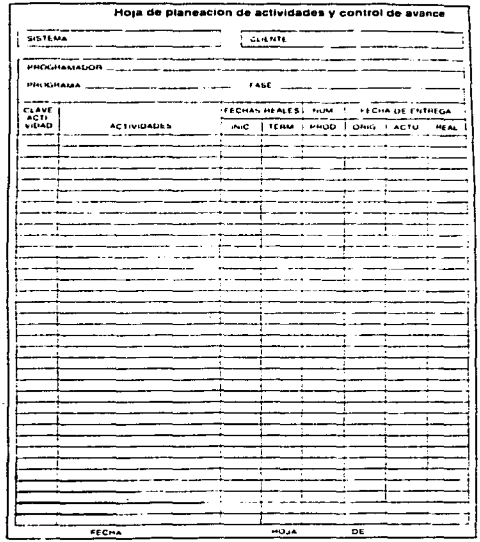


Figura III.16.- Control de Avance de Programación.


Hoja de planeacion de actividades y control de avance

SISTEMA
CLIENTE
PROGRAMADOR
PROGRAMA
FASE

CLAVE ACTIVIDAD	ACTIVIDADES	FECHAS REALES		NUM	FECHA DE ENTREGA		
		INIC	TERM	PROD	ORIG	ACTU	REAL

FECHA HOJA DE

Figura III.17.- Hoja de Planeación de Actividades y Control de Avance.

Etapa de programación.- Buscar la claridad, modalidad y verificar con base en las especificaciones.

Etapa de implementación y pruebas del sistema.- Desarrollar la implantación del sistema con datos de prueba y la carga de datos definitivos, evaluando el sistema, su seguridad y confidencialidad y dando entrenamiento a los usuarios. Las pruebas del sistema tratan de garantizar que se cumplan los requisitos de las especificaciones funcionales, verificando datos estadísticos, transacciones, reportes, archivos, anotando las fallas que pudieran ocurrir y realizando los ajustes necesarios. Los niveles de prueba pueden ser agrupados en módulos, programas y sistema total.

Esta función tiene una gran importancia en el ciclo de evaluación de aplicaciones delos sistemas de información y busca comprobar que la aplicación cumple las especificaciones del usuario, que se haya desarrollado dentro de lo presupuestado, que tenga los controles necesarios y que efectivamente cumpla con los objetivos y beneficios esperados.

Un cambio hecho a un sistema, como la creación de uno nuevo, presupone necesariamente cambios en la forma de obtener la información y un costo adicional. Ambos deberán ser evaluados. Se debe evaluar el cambio (si lo hay) de la forma en que se ejecutan las operaciones, se debe comprobar si mejora la exactitud de la información generada, si la obtención de los reportes efectivamente reduce el tiempo de entrega o si es más completa, (Piattini y del Peso, 1998).

Se debe determinar cuánto afecta las actividades del personal usuario o si aumenta o disminuye el personal de la Organización, así como los cambios entre las interacciones entre los miembros de la Organización. Todo ello, a fin de saber si aumenta o disminuye el esfuerzo realizado y su relación costo / beneficio para generar la información destinada a la toma de decisiones, con objeto de estar en condiciones de determinar la productividad y calidad del sistema.

Es muy frecuente que no se libere un sistema, esto es, que alguien continúe dándole mantenimiento y que sea el único que lo conozca. Ello puede deberse a amistad con el usuario, falta de documentación, mal análisis preliminar del sistema, resistencia a cambiar a otro proyecto, o bien a una situación que es muy grave dentro del área de Informática: la aplicación de *"indispensables"*, que son los únicos que tienen la información y, por lo tanto, son inamovibles.

¿Qué sucede respecto al mantenimiento de un sistema cuando éste no ha sido bien desarrollado (analizado, desarrollado, diseñado, probado, programado) e instalado? La respuesta es sencilla: necesitará cambios frecuentes por omisiones o nuevos requerimientos.

En el caso de sistemas, muchas organizaciones están gastando cerca de 80% de sus recursos de cómputo en mantenimiento. El mantenimiento excesivo es consecuencia de falta de planeación y control del desarrollo de sistemas; la planeación debe contemplar los recursos disponibles y técnicos apropiados para el desarrollo.

Por su parte, el control debe tener como soporte el establecimiento de Normas de desarrollo que han de ser verificados continuamente en todas las etapas del desarrollo de un sistema. Estas Normas no pueden estar aisladas, primero, del contexto particular de la Dirección de Informática (ambiente) y, segundo, de los lineamientos generales de la Organización, para lo cual es necesario contar con personal en desarrollo que posea suficiente experiencia en el establecimiento de Normas de desarrollo de sistemas. Estas mismas características deben existir en el personal de auditoría de sistemas. Es poco probable que un proyecto legue a un final feliz cuando se ha iniciado sin éxito. (Abrams y Jajodia, 1995).

El excesivo mantenimiento de los sistemas generalmente es ocasionado por un mal desarrollo. Esto se inicia desde que el usuario establece sus requerimientos (en ocasiones sin saber qué desea) hasta la instalación del sistema, sin que se haya establecido un plan de prueba de éste para medir su grado de confiabilidad en la operación que se efectuará.

Para verificar si existe esta situación, se debe pedir a los analistas las actividades que están desarrollando en el momento de la auditoría y evaluar si están efectuando actividades de mantenimiento o si se están realizando nuevos proyectos. En ambos casos se deberá evaluar el tiempo que llevan dentro del mismo sistema, la prioridad que se le asignó y cómo está el tiempo real en relación con el tiempo estimado en el plan maestro. El que los analistas, los programadores, o unos y otros, tengan acceso en todo momento a los sistemas puede ser un grave problema y ocasionar fallas de seguridad.

III.16.- Instrucciones de Operación.

Se debe evaluar los instructivos de operación de los sistemas para evitar que los programadores tengan acceso a los sistemas en operación. El contenido mínimo de los instructivos de operación deberá comprender:

- Diagrama de flujo por cada programa.
- Diagrama particular de entrada-salida.
- Mensaje y su explicación.
- Parámetros y su explicación.
- Diseño de impresión de resultados.

- Cifras de control.
- Fórmulas de verificación.
- Observaciones.
- Instrucciones en caso de error.
- Calendario de proceso y resultados.

III.17.- Forma de Implantación.

La finalidad es la de evaluar los trabajos que se realizan para iniciarse la operación de un sistema; esto comprende: prueba integral del sistema, adecuación, aceptación por parte del usuario, entrenamiento de los responsables del sistema. Para ello deben de considerarse los siguientes aspectos:

1.- Indicar cuáles puntos se toman en cuenta para la prueba de un sistema:

- Prueba particular de cada programa.
- Prueba por fase, validación, actualización.
- Prueba integral del paralelo.
- Prueba en sistema paralelo.
- Pruebas de seguridad y confidencialidad.
- Otros (especificar).

2.- En la implantación se debe de analizar la forma en que se van a cargar inicialmente los datos del sistema, lo cual puede ser por captura o por transferencia de información. Estos datos pueden ser de todo el sistema, o bien en forma parcial. Lo que es necesario evaluar es la forma en que se van a cargar las cifras de control o bien los datos acumulados.

3.- También se debe hacer un plan de trabajo para la implantación, el cual debe contener las fechas en que se realizarán cada uno de los procesos.

III.18.- Equipo y Facilidades de Programación.

La selección de la configuración de un sistema de cómputo incluye la interacción de numerosas y complejas decisiones de carácter técnico. El impacto en el rendimiento de un sistema de cómputo debido a cambios trascendentales en el Sistema Operativo o en el equipo, puede ser determinado por medio de un paquete de pruebas (*benchamark*) que haya sido elaborado para este fin en la Dirección de Informática. Es conveniente solicitar pruebas y comparaciones entre equipos (*bechamark*) para evaluar la situación del equipo y del *"software"* en relación con otros que se encuentran en el mercado.

III.19.- Entrevistas a Usuarios.

Las entrevistas se deberán llevar a cabo para comparar los datos proporcionados y la situación de la Dirección de Informática desde el punto de vista de los usuarios. Su objetivo es conocer la opinión que tienen los usuarios sobre los servicios proporcionados, así como la difusión de las aplicaciones del ordenador y de los sistemas en operación. Las entrevistas se deberán hacer, en caso de ser posible, a todos los usuarios o bien en forma aleatoria a algunos de ellos, tanto a los más importantes como a los de menor importancia en cuanto al uso del equipo.

Aunque la Entrevista es una de las fuentes de información más importantes para saber cómo opera un sistema, no siempre tiene la efectividad que se desea, ya que en ocasiones las personas entrevistadas pueden ser presionadas por los analistas de sistemas, o piensan que si hacen algunos cambios, éstos podrían afectar su trabajo. El Gerente debe de hacer del conocimiento de los entrevistados el propósito del estudio. Una guía para la entrevista puede ser la siguiente:

- Prepararse para la Entrevista estudiando los puestos de las personas que van a ser entrevistadas y sus funciones dentro de la Organización.
- Presentarse y dar un panorama del motivo de la Entrevista.
- Comenzar con preguntas generales sobre las funciones, la organización y los métodos de trabajo.
- Hacer preguntas específicas sobre los procedimientos que puedan dar como resultado el señalamiento de mejoras.
- Seguir los temas tratados en la Entrevista.
- Limitar el tomar notas a lo más relevante, para evitar distractores.
- Al final de la Entrevista, ofrecer un resumen de la información obtenida y preguntar cómo se le puede dar seguimiento.

III.20. Cuestionario.

El diseño de un cuestionario debe tener una adecuada preparación, elaboración, preevaluación y evaluación, (Echenique, 1998). Algunas guías generales son:

1.- Identificar el grupo que va a ser evaluado.
2.- Escribir una introducción clara, para que el investigado conozca los objetivos del estudio y el uso que se le dará a la información.
3.- Determinar qué datos deben ser recopilados.
4.- Elaborar las preguntas con toda precisión (no hacer preguntas en negativo), de tal forma que la persona que las responda lo pueda hacer con toda claridad. Estructurar las preguntas en forma lógica y secuencial de tal forma que el tiempo de respuesta y de escritura sea breve (aunque se deben dejar abiertas las observaciones). Eliminar todas aquellas preguntas que no tengan un objetivo claro, o que sean improcedentes.
5.- Limitar el número de preguntas para evitar que sea demasiado el tiempo de contestación y que se pierda el interés de la persona.
6.- Implementar un cuestionario piloto, para evaluar que todas las preguntas sean claras y que las respuestas sean las esperadas.
7.- Diseñar e implementar un plan de recolección de datos.
8.- Determinar el método de análisis que será usado.
9.- Distribuir los cuestionarios y darles seguimiento para obtener las respuestas deseadas; así mismo, analizar los resultados.

Procurar que el cuestionario responsa a las siguiente preguntas:

- ¿Qué áreas pueden ser mejoradas?
- ¿Qué información se necesita que actualmente no se tiene o que es difícil de obtener?
- ¿Qué *"cuellos de botella"* ocurren durante el día?, ¿Cómo se pueden eliminar?
- ¿Cómo se puede cambiar el procedimiento para eliminarlos?
- ¿Existe un procedimiento que sea redundante o repetitivo?
- ¿Cómo se podría eliminar esta repetición?

Desde el punto de vista del usuario los sistemas deben:

1.- Cumplir con los requerimientos totales del usuario.
2.- Cubrir todos los controles necesarios.
3.- No exceder las estimaciones del presupuesto inicial, en tiempo y costo.
4.- Ser fácilmente modificables.
5.- Ser confiables y seguros.
6.- Poderlos usar a tiempo, y con el menor tiempo y esfuerzo posible.
7.- Ser amigables.

Para que un sistema cumpla con los requerimientos del usuario no necesita una comunicación completa entre éste y el responsable del desarrollo del sistema. En ella se deben definir claramente los elementos con que cuenta el usuario, las necesidades del proceso de información y los requerimientos de información de salida, almacenada o impresa.

En esta misma etapa debió haberse definido la calidad de la información que será procesada por el ordenador, estableciéndose los riesgos de la misma y la forma de minimizarlos. Para ello se debieron definir os controles adecuados, estableciéndose además los niveles de acceso a la información; es decir, quién tiene privilegio de consultar, modificar o incluso borrar información.

Esta etapa deberá de ser cuidadosamente verificada por el auditor interno especialista en sistemas y por el auditor en Informática, para comprobar que se logró una adecuada comprensión de los requerimientos del usuario y un control satisfactorio de información. Para verificar si los servicios que se proporcionan a los usuarios son los requeridos y que se están proporcionando en forma adecuada, cuando menos será preciso considerar la siguiente información:

- Descripción de los servicios prestados.
- Criterios que utilizan los usuarios para evaluar el nivel del servicio prestado.
- Reporte periódico del uso y concepto del usuario sobre el servicio.
- Registro de los requerimientos planteados por el usuario.
- Tiempo de uso.

A continuación se presenta una guía de cuestionario para aplicarse durante la Entrevista con el Usuario:

1. ¿Considera que la dirección de informática le da los resultados esperados? SI NO

¿Por qué?

2. ¿Como considera usted, en general, el servicio proporcionado por la dirección de informática?

A. Deficiente B. Aceptable C. Satisfactorio D. Excelente

¿Por qué?

3. ¿Cubre sus necesidades de procesamiento?

A. No las cubre B. Parcialmente C. La mayor parte D. Todas

¿Por qué?

4. ¿Como considera la calidad del procesamiento que se le proporciona?

A. Deficiente B. Aceptable C. Satisfactorio D. Excelente

¿Por qué?

5. ¿Hay disponibilidad de procesamiento para sus requerimientos?

A. Generalmente no existe B. Ocasionalmente

C. Regularmente D. Siempre

¿Por qué?

6. ¿Conoce los costos de los servicios proporcionados? SI NO

7. ¿Que opina del costo del servicio proporcionado por el departamento de procesos electrónicos?

A. Excesivo B. Mínimo C. Regular D. Adecuado E. No lo conoce

¿Por qué?

8. ¿Son entregados con puntualidad los trabajos?

A. Nunca B. Rara vez C. Ocasionalmente

D. Generalmente E. Siempre

¿Por que?

9. ¿Que piensa de la presentacion de los trabajos solicitados?

A. Deficiente B. Aceptable C. Satisfactoria D. Excelente

¿Por que?

10. ¿Que piensa de la atencion brindada por el personal de procesos electrónicos?

A. Insatisfactoria B. Satisfactoria C. Excelente

¿Por que?

11. ¿Que piensa de la asesoria que se imparte sobre informatica?

A. No se proporciona B. Es insuficiente

C. Satisfactoria D. Excelente

¿Por que?

12. ¿Que piensa de la seguridad en el manejo de la informacion proporcionada para su procesamiento?

A. Nula B. Riesgosa C. Satisfactoria

D. Excelente E. Lo desconoce

¿Por que?

13. ¿Existen fallas de exactitud en los procesos de informacion? SI NO

¿Cuales?

14. ¿Como utiliza los reportes que se le proporcionan?

15. ¿Cuales no utiliza?

18. De aquellos que no utiliza, ¿por que razon los recibe?

17. ¿Que sugerencias hace en cuanto a la eliminacion de reportes: modificacion, fusion, division de reporte?

18. ¿Se cuenta con un manual del usuario por sistema? Si No

19. ¿Es claro y objetivo el manual del usuario? Si No

20. ¿Que opinion tiene sobre el manual?

NOTA: Pida el manual del usuario para evaluarlo

21. ¿De su departamento, quien interviene en el diseño de sistemas?

22. ¿En que sistemas tiene actualmente su servicio de computacion?

23. ¿Que sistemas desearia que se incluyeran?

24. Observaciones.

III.21.- Derechos de Autor y Secretos Industriales.

En relación con las disposiciones jurídicas adecuadas para la actividad Informática; la Cámara de Diputados y el Instituto Nacional de Estadística, Geografía e Informática (INEGI), organizaron un foro de consulta sobre Derecho e Informática. Como resultado se recopilaron opiniones, propuestas y experiencias relacionadas con diversos aspectos, entre los que destacan: las garantías para la información personal almacenada en bases de datos y la protección jurídica de datos de carácter estratégico; la tipificación de delitos informáticos; el valor probatorio del documento electrónico, y la protección de derechos de autor para quienes desarrollan programas para Ordenador, (Acha, 1994).

Dentro del concepto de propiedad intelectual, uno de los aspectos más importantes es el que se refiere a los derechos de autor, el cual involucra la parte más importante del desarrollo intelectual de las personas, ya que se refiere a las ramas literaria, científica, técnica, jurídica, musical, pictórica, escultórica, arquitectónica, fotográfica, cinematográfica, televisiva; así como los programas de cómputo, las Bases de Datos y los medios de comunicación, entre las más importantes.

En la mayoría de los países existen leyes protectoras de las obras intelectuales que producen los poetas, los novelistas, los compositores, los pintores, los escultores, y de manera reciente se han protegido, los programas de computadora y las Bases de Datos. Pero además de su legislación doméstica, las naciones celebran compromisos unas con otras para dar una protección internacional a los autores. En general, se admite que son cinco las razones de la protección.

En primer lugar, por una razón de justicia social: el autor debe obtener provecho de su trabajo. Los ingresos que perciba, deben estar en función de la acogida del público a sus obras y de sus condiciones de explotación: *"las regalías"* son, en cierto modo, los salarios de los trabajadores intelectuales.

En segundo, por una razón de desarrollo cultural; si está protegido, el autor se verá estimulado para crear nuevas obras, enriqueciendo de esta manera la literatura, el teatro, la música, los programas de computación elaborados en su país. Nadie debe realizar un trabajo sin que sea debidamente remunerado; del mismo modo, los que, por su trabajo, su inteligencia, su experiencia, contribuyendo a la elaboración de programas y sistemas de cómputo, deben de ser debidamente remunerados.

En tercero, por una razón de orden económico; las inversiones que son necesarias, por ejemplo, para la elaboración de un sistema de cómputo serán más fáciles de obtener si existe una protección efectiva.

En cuarto, por una razón de orden moral; al ser la obra la expresión personal del pensamiento del autor, éste debe tener derecho a que se respete, es decir; derecho a decidir si puede ser reproducida o ejecutada en público, cuándo y cómo, y derecho a oponerse a toda deformación o mutilación cuando se utiliza la obra.

En quinto lugar, por una razón de prestigio nacional: el conjunto de las obras de los autores de un país refleja el alma de la nación y permite conocer mejor sus costumbres, sus usos, sus aspiraciones. Si la protección no existe, el patrimonio cultural será escaso y no se desarrollarán las artes.

El programa de computación, conocido en inglés como *"Computer Program"* y en francés *"Programe d' Ordinateur"*, y también llamado Programa de Ordenador (en Castellano); es un conjunto de instrucciones que cuando se incorpora a un soporte legible por máquina, puede hacer que una máquina con capacidad para el tratamiento de la información indique, realice o consiga una función, tarea o resultados determinados.

Cada vez se acepta con mayor frecuencia que los programas originales son obras creadoras a la protección que otorga el Derecho de Autor. Una de las últimas adiciones de que fue objeto la precedente ley autoral, consistió en incorporar entre las obras protegidas a los programas de computación.

Artículo 11.- El derecho de autor es el reconocimiento que hace el Estado a favor de todo creador de obras literarias y artísticas previstas en el artículo 13 de esta Ley, en virtud del cual otorga su protección para que el autor goce de prerrogativas y privilegios exclusivos de carácter personal y patrimonial.

La legislación actual, además de conservar dichos programas en un similar catálogo de las obras para las que se reconocen los derechos de autor (artículo 13, LFDA), les dedica un capítulo especial (capítulo IV del título IV) con reglas particulares también sobre protección). Ley Federal de Derechos de Autor (2000).

Artículo 13. Los derechos de autor a que se refiere esta Ley se reconocen respecto de las obras de las siguientes ramas:

[...]

XI. Programas de Cómputo;

[...]

Las demás obras que por analogía puedan considerarse obras literarias o artísticas se incluirán en la rama que les sea más afín a su naturaleza.

Artículo 83. Salvo pacto en contrario la persona física o moral que comisione la producción de una obra o que la produzca con la colaboración remunerada de otra, gozará de la titularidad de los derechos patrimoniales sobre la misma y le corresponderán facultades relativas a la divulgación, integridad de la obra y de colección sobre este tipo de creaciones.

La persona que participe en la realización de la obra, en forma remunerada, tendrá el derecho a que se le mencione expresamente su calidad, de autor, artista, intérprete o ejecutante sobre la parte o partes en cuya creación haya participado.

Artículo 84. Cuando se trate de una obra realizada como consecuencia de una relación laboral establecida a través de un contrato individual de trabajo que conste por escrito, a falta de pacto en contrario, se presumirá que los derechos patrimoniales se dividen por partes iguales entre empleador y empleado. El empleador podrá divulgar la obra sin autorización del empleado, pero no al contrario. A falta de contrato individual de trabajo por escrito, los derechos patrimoniales corresponderán al empleado.

Capítulo IV

DE LOS PROGRAMAS DE COMPUTACIÓN Y BASES DE DATOS.

Artículo 101. Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, en un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

Artículo 102. Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código, fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

Artículo 103. Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste. Con excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

Artículo 104. Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa o sobre una base de datos conservará aun después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

El Artículo 105. El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

I. Sea indispensable para la utilización del programa, o
II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

Artículo 106. El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio o forma;
II.- La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;
III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y
IV. La descompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

Artículo 107. Las Bases de Datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

Artículo 108. Las Bases de Datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

Artículo 109. El acceso a información de carácter privado relativa a las personas contenida en las Bases de Datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate. Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la Ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Artículo 110. El titular del derecho patrimonial sobre una Base de Datos tendrá derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;

II. Su traducción, adaptación, reordenación y cualquier otra modificación;

III. La distribución del original o copias de la Base de Datos;

IV. La comunicación al público, y

V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111. Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

Artículo 112. Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

Artículo 113. Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.

Artículo 114.- La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite y otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

Artículo 231. Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto:

I. Comunicar o utilizar públicamente una obra protegida por cualquier medio, y de cualquier forma, sin la autorización previa y expresa del autor, de sus legítimos herederos o del titular del derecho patrimonial del autor;

II. Utilizar la imagen de una persona sin su autorización o la de sus causahabientes;

III. Producir, reproducir, almacenar, distribuir, transportar o comercializar copias de obras, fonogramas, videogramas o libros protegidos por los derechos de autor o por los derechos conexos, sin la autorización de los respectivos titulares en términos de esta Ley;

IV. Ofrecer en venta, almacenar, transportar o poner en circulación obras protegidas por esta Ley que hayan sido deformadas, modificadas o mutiladas sin autorización del titular del derecho de autor.

V. Importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

VI. Retransmitir, fijar, reproducir y difundir al público emisiones de organismos de radiodifusión y sin la autorización debida, y

VII. Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular.

Artículo 232. Las infracciones en materia de comercio previsto en la presente Ley serán sancionadas por el Instituto Mexicano de la Propiedad Industrial con multa:

I. De cinco mil hasta diez mil días de salario mínimo en los casos previstos en las fracciones I, III, IV, V, VII, VIII y IX del artículo anterior;

II. De mil hasta cinco mil días de salario mínimo en los casos previstos en las fracciones II y VI del artículo anterior, y

III. De quinientos hasta mil días de salario mínimo en los demás casos a que se refiere la fracción X del artículo anterior.

Se aplicará multa adicional de hasta quinientos días de salario mínimo general vigente por día a quien persista en la infracción.

Artículo 233. Si el infractor fuese un editor, organismo de radiodifusión, o cualquier persona física o moral que explote obras a escala comercial, la multa podrá incrementarse hasta en un cincuenta por ciento respecto de las cantidades previstas en el artículo anterior.

III.22.- Internet.

El Internet, considerado como una colección de redes interconectadas o como un conjunto de ordenadores unidos entre sí, no ha sido tomado en cuenta entre las disposiciones que se acaban de mencionar.

Para obtener acceso a Internet se requiere un equipo que está alcance del público en general, por lo que cualquier persona puede entrar a la *"Red de Redes de Comunicación"* si contrata los servicios de un proveedor de acceso.

Recientemente han surgido empresas proveedoras de servicios dedicados a ofrecer en renta conexiones a Internet, ya sea de manera directa, indirecta o parcial, siendo las propias empresas las que proporcionan el equipo necesario para tener acceso.

Los proveedores de servicios son los responsables de la información que ponen al servicio de sus usuarios, ya que dichas compañías son encargadas de divulgar y controlar la información transmitida por Internet.

Son muy complejos los aspectos técnicos que implica conocer las acciones llevadas a cabo en Internet para determinar cuáles pudieran constituir alguna infracción a los derechos de autor. No obstante, se puede pensar que este sistema de comunicaciones puede originar las siguientes violaciones: al derecho moral de modificar la obra; al derecho moral inédito; al derecho de publicar obra bajo el propio nombre o de manera anónima, (Alonso, 1989).

También puede producirse violaciones a los derechos patrimoniales cuando se transmiten obra intelectuales en forma de archivos por medio de Internet, ya que realiza una utilización pública de una obra sin la remuneración para el autor de la creación intelectual.

También puede ser fácilmente violado el derecho de autor cuando la red utiliza la propia imagen, de la que son titulares los artistas, intérpretes y ejecutantes, por cuanto que en Internet es posible encontrar un gran número de imágenes que pueden ser reproducidas imprimiéndolas sobre papel, como carteles, o sobre tela para obtener prendas de vestir (como playeras con la imagen del artista preferido).

El debate sobre la protección de los datos personales en Internet reabre la polémica sobre el papel desempeñado por los *"cookie"* [1], que sirven más como instrumento de mercadotecnia que como medio para espiar a los usuarios de Internet, (Arkin, 2000).

Cuando un visitante accede una página *web* por primera vez, el servidor le atribuye generalmente un número de identificación con atributos, el *"cookie"*. Después, extrae su nombre de un fichero empleado en las plataformas UNIX, los *"magic cookies"*, con lo que el visitante será identificado en sus visitas ulteriores.

Esto permite al propietario de la página analizar el comportamiento de sus visitantes y personalizar sus visitas. El desplazamiento de los usuarios de Internet entre varias páginas de una dirección se puede identificar a la perfección, lo que permite *"tomar nota"* del recorrido utilizado más a menudo. La dirección electrónica podrá ser modificada para satisfacer a la vez al visitante y a los anunciantes, que pueden colocar su publicidad en el lugar más adecuado.

El *"cookie"* sirve también para grabar lo que ocurre en estas visitas, sobre todo en caso de compra. Si se elige, por ejemplo, un libro en una librería en línea, la compra queda grabada en un *"cookie"*, antes de reaparecer en el momento de pagar la factura en la caja virtual. La visita también puede ser personalizada grabando en el archivo *"cookie"* las informaciones facilitadas por el usuario.

Teóricamente la seguridad de estas informaciones está garantizada, ya que un servidor sólo puede obtener la información del *"cookie"* que ha producido. Las redes de publicidad en línea si tienen esta capacidad. Estas innovaciones han alarmado algunas asociaciones, para quienes este sistema supone una verdadera intrusión en la vida privada de los usuarios de Internet.

[1] El término *"cookie"* se aplica a un simple archivo de datos situado en el disco duro del Ordenador de una persona o Compañía que ofrece servicios de Internet. El *"cookie"* y su contenido son creados por un servidor que almacena una o varias páginas Internet.

Esta captación de datos se realiza sin que el usuario lo sepa, a menos que haya configurado su Navegador para ser advertido. Los que no disponen de este sistema pueden borrar periódicamente el fichero *"cookie"* de su disco duro o recurrir a un programa especial. La situación de los *"cookies"* debe ser evaluada dentro de la Auditoría, para determinar si se considera una intromisión la privacidad de los usuarios de Internet de una Compañía.

III.23.- Protección de los Derechos de Autor.

Las obras protegidas por la Ley deberán ostentar la expresión "Derechos Reservados" o su abreviatura D.R., seguida por el símbolo ©. Sin embargo, la omisión de estos requisitos no implica la pérdida de los derechos de autor, aunque sujeta al responsable a las sanciones establecidas en la Ley. (IFIP, 1990).

La reserva de los derechos de autor es la facultad para usar y explotar en forma exclusiva títulos, nombres, denominaciones, características físicas y psicológicas distintivas o características de operación originales. Ahora bien, para proteger los derechos de autor se han establecido diversos procedimientos, el primero relacionado con los delitos que pueden cometerse al invadirse un derecho de autor, por lo cual se estableció el artículo 215 de la Ley de Derechos Autor, que corresponde conocer a los tribunales de la Federación, sobre los delitos relacionados con el derecho del autor, los cuales deberán estar previstos en el Código Penal para el Distrito Federal, que regula los delitos en materia del fuero común y para toda la República Mexicana en materia del fuero federal.

Independientemente de solicitar el ejercicio de la acción penal, la persona afectada por un derecho protegido por la Ley de Derechos de Autor, podrá optar entre hacer valer las acciones judiciales que le correspondan o sujetarse al procedimiento de avenencia. Éste, tiene por objetivo dirimir de manera amigable un conflicto surgido con motivo de la interpretación o aplicación de la Ley, y se inicia con la queja, que se presenta directamente ante el Instituto Nacional del Derecho de Autor.

Mediante la aplicación del artículo 2° de la Ley de Derechos de Autor, corresponde al Instituto Nacional del Derecho de Autor su aplicación administrativa, y en los casos previstos por dicha Ley a el Instituto Mexicano de la Propiedad Industrial. Mediante el arbitraje, las partes podrán resolver todas las controversias que hayan surgido en materia de derechos de autor, y podrán someterse por medio de cláusula compromisoria o compromiso arbitral.

Es de señalar que el artículo 223 de la Ley de Derechos de Autor señala que para ser árbitro se requiere ser licenciado en Derecho, pero no es requisito el ser especialista en el área en que se va arbitrar, como sería el ser experto en programación, Informática o Bases de Datos. Las penalidades en caso de delitos se han incrementado notablemente de acuerdo con lo señalado en el:

CÓDIGO PARA EL DISTRITO FEDERAL EN MATERIA DE FUERO COMÚN Y PARA TODA LA REPÚBLICA EN MATERIA DE FUERO FEDERAL.

"TÍTULO VIGÉSIMO SEXTO"
DE LOS DELITOS EN MATERIA DE DERECHOS DE AUTOR.

Artículo 424. Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días de multa de salario mínimo vigente:

I. Al que especule en cualquier forma con los libros de texto gratuitos que distribuye la Secretaría de Educación Pública;

II. Al editor, producto o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la Ley Federal del Derecho de Autor, que los autorizados por el titular de los derechos;

III. A quien produzca, reproduzca, importe, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros protegidos por la Ley Federal de Derechos de Autor, en forma dolosa; a escala comercial y sin la autorización que en los términos de la citada Ley debe otorgar al titular de los derechos de autor o delos derechos conexos;

IV. Las mismas sanciones se impondrán a quien use en forma dolosa, a escala comercial y sin la autorización correspondiente, obras protegidas por la mencionada ley, y;

V. A quien fabrique con fines de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Artículo 425. Se impondrá prisión de seis meses a dos años o de trescientos a tres mil días de multa, al que a sabiendas y sin derecho explote con fines de lucro una interpretación o una ejecución.

Artículo 426. Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días de multa, en los siguientes casos:

I. A quien fabrique, importe, venda, arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal, y

II. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.

Artículo 427. Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días de multa, a quien publique a sabiendas una obra sustituyendo el nombre del autor por otro nombre.

Artículo 428. Las sanciones pecuniarias previstas en el presente título se aplicarán sin perjuicio de la reparación del daño, cuyo monto no podrá ser menor al cuarenta por ciento del precio de venta al público de cada producto o de la presentación de servicios que impliquen violación a alguno o algunos de los derechos tutelados por la Ley Federal del Derecho de Autor.

Artículo 429. Los delitos previstos en este título se perseguirán por querella de la parte ofendida, salvo el caso previsto en el artículo 424, fracción I, que será perseguido de oficio.

III. 24.- Secretos Industriales.

III.24.1.- Artículos de la Ley de la Propiedad Industrial en Materia de Secretos Industriales.

Artículo 82. Se considera secreto industrial toda información de aplicación industrial o comercial que guarde una persona física o moral con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros en la relación de actividades económicas y respecto de la cual haya adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma. La información de un secreto industrial necesariamente deberá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción o a los medios o formas de distribución o comercialización de productos o prestación de servicios.

No se considerará secreto industrial aquella información que sea del dominio público la que resulte evidente para un técnico en la materia, con base en información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial. No se considerará que entra al dominio público o que es divulgada por disposición legal aquella información que sea proporcionada a cualquier autoridad por una persona que la posea como secreto industrial, cuando la proporción es para el efecto de obtener licencias, permisos, autorizaciones, registros, o cualquiera otros actos de autoridad.

Se considera secreto industrial "toda información de aplicación industrial o comercial". En principio, respecto de la aclaración de que la información puede ser de carácter industrial o comercial, la cual, aun y cuando parece elemental, daba lugar a que en ciertos casos la voluntad del legislador pretendiera interpretarse en un sentido restrictivo, limitando la protección exclusivamente a la información estrictamente de carácter industrial.

Por otro lado, especial peso debe concederse al término "aplicación" que incluye el precepto al referirse a los secretos industriales, ya que la información deberá satisfacer ese particular requisito. De hecho, en este punto se puede encontrar una relativa equivalencia con el requisito que al efecto se establece en materia de patentes, consistente en que las intervenciones sean susceptibles de aplicación industrial.

Es claro que la expresión "aplicable", en este particular contexto, debe ser interpretada en su forma más amplia, ya que pudiera presentarse el caso de que cierta información que aun y cuando en la práctica aún no hubiese sido puesta en práctica, sus posibilidades de ser implantada le ubiquen como información merecedora de la tutela de este régimen.

En aras de que el régimen tutelar de los secretos industriales verdaderamente constituya un medio de protección de información confidencial que se estima como bien económicamente valioso, la limitación que el precepto realiza del tipo de información que califica como constitutiva de secretos industriales, incorpora la palabra "referida a", con lo que el legislador parece establecer que basta que la información guarde cierta liga o esté asociada a las actividades fundamentales del agente económico o bien una ventaja competitiva para poder ser considerada como apta para constituir un secreto industrial, lo cual puede ser cuestionable, ya que no todas las copias, por ejemplo, de programas, tienen una finalidad de beneficio económico o una ventaja competitiva.

Entre la información tipicamente considerada como constitutiva de secretos industriales se cuenta la relativa a listas de clientes y proveedores, formulaciones, procesos industriales, estrategias de mercado, lanzamiento de productos, resultados de estudios comerciales y de mercado, sueldos, procesos legales, listas de precios, bases de datos, y en general, cualquier información sensible que represente un valor económico para la Empresa, este tipo de información se puede considerar directamente ligada con bases de datos.

Respecto de la condición de que el secreto industrial sea guardado por una persona física o moral con carácter confidencial, puede considerarse que sin duda constituye ésta el núcleo fundamental que imprime a este tipo de información la característica que le califica como secreto industrial.

Es importante considerar que el precepto no establece condición alguna respecto del origen de la información que guarda su poseedor; es decir, no se establece como condición el que la información hubiese sido generada por su poseedor, o bien, que la misma hubiese sido obtenida por algún título legal como pueda ser su transmisión por parte de un tercero, por lo que la información contenida en una base de datos, es considerada como un secreto industrial, sin importar si ésta fue o no creada por la persona que la posee y que la puedan difundir.

Obviamente, se abre aquí el planteamiento de si la información que eventualmente ha sido obtenida de manera ilegal, en caso de seguir cumpliendo las condiciones de confidencialidad exigidas por el precepto, debe ser merecedora de la protección conferida a los secretos industriales. Sería el caso, por ejemplo, de información que indebidamente revele un ex empleado a su nuevo patrón, y que éste pretenda conservar y proteger como secreto industrial propio, o bien copias de programas que posea un empleado y que las proporcione a su nuevo empleador.

En términos del tercer párrafo ce este mismo artículo, se establece que no se considera que entra al dominio público o que es divulgada por disposición legal aquella información que se a proporcionada a cualquier autoridad por una persona que la posea como secreto industrial, cuando se proporcione para el objeto de obtener licencias, permisos, autorizaciones, registros o cualesquiera otros actos de autoridad.

Las bases de datos que son del dominio público, pero que son modificadas, mejoradas o ampliadas, para lo cual se emplean tiempo y recursos, se convierten en propiedad industrial. Es el caso, por ejemplo, de múltiples bases de datos son obtenidas a partir de información accesible para el público, pero que al imprimirse una dosis significativa de recursos, tiempo y talento, la información es tratada y depurada hasta el grado de convertirla en un producto nuevo y diferente, que por ese sólo hecho merece que la legislación confiere a los secretos industriales, siempre que, desde luego, se satisfagan las otras condiciones exigidas para esta figura.

Este mismo criterio puede aplicarse a ciertos programas de computación que para su conformación han requerido de la participación de especialistas que han invertido en la investigación cantidades notables de esfuerzo y erudición, de manera que el resultado puede ser considerado como secreto industrial.

Un aspecto que es conveniente destacar es que en este punto la disposición parece adaptarse del texto del Tratado de Libre Comercio de América del Norte (TLCAN), en su artículo 1711, únicamente requiere que quien posee el secreto hubiere tomado "medidas a su alcance". El punto parece mínimo, pero es claro que existe una gran distancia entre haber tomado "medidas al alcance" que haber tomado "las medidas necesarias", tal como la Ley de Propiedad Industrial lo determina.

Resulta imprescindible para las empresas modernas con un reglamento interno de trabajo, en el que se especifiquen las políticas de la Empresa en materia de información confidencial. Dicho reglamento debe ser conocido por todos los empleados y funcionarios de la Empresa, y su puesta en práctica debe ser un asunto prioritario para cumplir con los requerimientos que la Ley determina para la constitución y preservación del secreto industrial. Entre las políticas que deben observarse como mínimas en materia de secretos industriales se cuentan enunciativamente las consistentes en la identificación de los materiales considerados como secreto de negocios, la prohibición de la duplicación de documentos sensibles sin autorización, el control de ingreso a las áreas en que la información se concentra, la utilización de sistemas de seguridad y control, la implantación de claves de acceso a los ordenadores, la firma de convenios de confidencialidad con empleados y proveedores, etcétera. Estos puntos son tratados con mayor amplitud en el tema relacionado a la seguridad.

Entre otras disposiciones aplicables se encuentran las de la Ley Federal de Responsabilidades de los Servidores Públicos, que en su artículo 47 determina que todo servidor público tendrá la obligación e custodiar y cuidar la documentación e información que por razón de su empleo, cargo o comisión, conserve bajo su cuidado o a la cual tenga acceso, impidiendo o evitando el uso, la sustracción, destrucción, ocultamiento o inutilización indebida de la misma.

En relación con el llamado "know how", cabe también hacer la distinción de que no toda la información de este tipo es necesariamente confidencial, ya que este concepto de dirige a referir aquel conjunto de conocimientos y habilidades que permiten a una persona o grupo de personas desarrollar, producir, distribuir o comercializar un bien o un servicio con ventajas frente a otros competidores, pero con la característica de que dicha información bien puede estar en el dominio público, y en su caso son elementos como la experiencia y la destreza lo que permite consolidar la ventaja de ese "saber hacer". Es decir, en el caso del "know how" se puede considerar que una de sus diferencias básicas con los secretos industriales es que no necesariamente es información que deba considerarse como confidencial. La definición de la "Uniform Trade Secrets Act", legislación que en los Estados Unidos de América habla sobre los secretos industriales es la siguiente:

"Un secreto industrial podrá consistir en cualquier fórmula, patrón, dispositivo o compilación de información que se usen en una Empresa y que den al empresario la oportunidad de obtener una ventaja sobre los competidores que no lo conocen o no lo usan. Puede ser la fórmula de un compuesto químico, un proceso de manufactura, de tratamiento o de conservación de materiales, el patrón para una máquina u otro dispositivo, o una lista de clientes".

Artículo 83. La información a que se refiere el artículo anterior, deberá constar en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros instrumentos similares. Es importante considerar que este precepto adiciona un elemento más, y es el hecho de que la información respectiva debe constar en un soporte material. Un problema que se tiene está en que para que los documentos que contienen el secreto industrial sean registrados ante el Registro Nacional de Derecho de Autor, dependiente de el Instituto Nacional del Derecho de Autor, deben ser presentados en un soporte material, y al tratarse de un registro público las hace accesible a terceros perdiendo, precisamente por ese hecho, cualquier tipo de protección legal que como secreto industrial le hubiere correspondido.

Artículo 84. La persona que guarde un secreto industrial podrá transmitirlo o autorizar su uso a un tercero. El usuario tendrá la obligación de no divulgar el secreto industrial por ningún medio. En los convenios por los que se transmitan conocimiento técnico, asistencia técnica, provisión de ingeniería básica o de detalle, se podrán establecer cláusulas de confidencialidad para proteger los secretos industriales que contemplen, los cuales deberán precisar los aspectos que comprenden como confidenciales.

Artículo 85. Toda aquella persona que, con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a un secreto industrial del cual se haya prevenido sobre su confidencialidad, deberá abstenerse de revelarlo sin causa justificada y sin consentimiento de la persona que guarde dicho secreto, o de su usuario autorizado. Todas las personas mencionadas en el precepto parecen cubrir las diversas opciones de quienes pueden tener legal acceso a los secretos industriales de su poseedor, esto es, trabajadores, empleados, asesores, y en general, cualquiera que tenga acceso a los secretos por virtud de sostener una relación de negocios con el que guarda el secreto. De acuerdo con las fracciones III, IV y V del artículo 223 de la Ley de Propiedad Industrial, no sólo la revelación del secreto está vedada, sino también su utilización y aprovechamiento.

Artículo 86. La persona física o moral que contrate a un trabajador que esté laborando o haya laborado o a un profesional, asesor o consultor que preste o haya prestado sus servicios para otra persona, con el fin de obtener secretos industriales de ésta, será responsable del pago de daños y perjuicios que le ocasione a dicha persona. También será responsable del pago de daños y perjuicios la persona física o moral que por cualquier medio lícito obtenga información que contemple un secreto industrial.

El artículo 223 de la Ley de Propiedad Industrial define y sanciona las conductas delictivas en relación con secretos industriales. Al propio tiempo, el artículo incurre en otra intrascendencia por obviedad, al señalar que quien reciba secretos industriales de terceros por vía de contratar a sus empleados o ex empleados, asesores o ex asesores, será responsable de los daños y perjuicios que ocasiones, siendo que dicha obligación deviene de cualquier hecho, ilícito que lesione a una persona, tal como lo prescribe el artículo 1910 de el Código Civil.

III.24.2.- Consideraciones Legales sobre el Empleo de Nombres de Dominio Frente al Régimen de Marcas.

Las posibilidades de la comunicación vía Internet son inagotables, comprendiéndose dentro de ellas la posibilidad de ofertar productos y prestar servicios al enorme mercado potencial que acude a los sitios en la Red, mediante la obtención de un nombre de dominio que refiera a los usuarios de la red a un sitio exclusivo destinado a promover sus bienes y / o servicios.

Los nombres de dominio son denominaciones únicas asignadas a personas que desean tener un domicilio que pueda ser visitado por usuarios de la Red. El sistema de dominio interpreta los nombres como números y cada ordenador conectado a la red cuenta con un número único.

La concesión de nombres de dominio es coordinada por un organismos llamado **Network Solutions Inc**, a través de ***InterNIC***, quien trabaja en conjunto con administradores de dominio, coordinadores de redes y proveedores de servicio de Internet. Los nombres de dominio son registrados a través de una forma de solicitud estándar disponible en la red y el único criterio seguido para su concesión es el de verificar que no exista un nombre de dominio idéntico, previamente asignado. Lo anterior, resulta necesario desde el punto de vista técnico, ya que no pueden existir dos rutas de acceso idénticas de sitios distintos en la red. El comercio de bienes y servicios a través de la Red ha propiciado la confrontación de los intereses de titulares de marcas registradas con dueños de sitios en la red que adoptan marcas propiedad de terceros como nombres de dominio.

Desde fines de 1995, los gobiernos de los estados y distintas organizaciones internacionales han encaminado sus esfuerzos a balancear de manera adecuada, por un lado, la necesidad de proteger los derechos de propiedad intelectual y, por otro, las innegables ventajas del acceso a la información vía Internet.

Mantiene el liderazgo de dicha Empresa *Network Solutions, Inc (NSI)*, que es el brazo operativo de la *US National Science Foundation*, autoridad que regula la asignación de dominios en Internet.

En el Décimo Congreso de las Naciones Unidas sobre previsión del delito y tratamiento del delincuente celebrado en Viena, Austria del 10 al 17 de Octubre del 2000, se llegó a la conclusión sobre los delitos relacionados con las redes informáticas: *"Para combatir eficazmente los delitos cibernéticos es necesario un enfoque internacional coordinado a diferentes niveles. A nivel nacional, la investigación de esos delitos requiere personal, conocimientos especializados y procedimientos adecuados. Se alienta a los Estados a que consideren la posibilidad de crear mecanismos que permitan obtener de manera oportuna datos exactos de los sistemas y redes informáticas cuando estos datos se requieran como prueba en los procedimientos judiciales. A nivel internacional, la investigación eficaz de los delitos cibernéticos requiere una adecuación oportuna, facilitada por la coordinación entre los organismos nacionales de aplicación de la Ley y la institución de la autoridad legal pertinente".*

CAPÍTULO IV.

AUDITORÍA DE LA SEGURIDAD EN REDES.

IV.1.- Introducción.

Los ordenadores son un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

Esta información puede ser de suma importancia, y no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Ante esta situación, en el transcurso de este siglo el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y derecho.

Imaginese que, por una u otra razón, el Centro de Cómputo o las librerías son destruidos o usados inapropiadamente, ¿cuánto tiempo pasaría para que esta Organización estuviese nuevamente en operación? El centro de cómputo puede ser el activo más valioso y al mismo tiempo, el más vulnerable. En la situación actual de criminología, en los delitos de *"cuello blanco"* se incluye la modalidad de los delitos hechos mediante el ordenador o los sistemas de información, de los cuales el 95% de los detectados han sido descubiertos por accidente, y la gran mayoría no han sido divulgados para evitar dar ideas a personas mal intencionadas. Es así como el Ordenador ha modificado las circunstancias tradicionales del crimen. Muestra de ello son los fraudes, falsificaciones y venta de información hechos a los Ordenadores o por medio de éstas, (Almela, 2002).

Existen diferentes estimaciones sobre el costo de los delitos de *"cuello blanco"*, las cuales dependerán de la fuente que haga estas estimaciones, pero en todos los casos se considera que los delitos de *"cuello blanco"* en los Estados Unidos de América superan los miles de millones de dólares.

Durante mucho tiempo se consideró que los procedimientos de auditoría y seguridad eran responsabilidad de la persona que elabora los sistemas, in considerar que son responsabilidad del área de Informática en cuanto a la elaboración de los sistemas del usuario en cuanto a la utilización que se le dé a la información y a la forma de acceder a ella, y del Departamento de Auditoría Interna en cuanto a la supervisión y diseño de los controles necesarios. La seguridad del área de Informática tiene como objetivos:

- Proteger la integridad, exactitud y confidencialidad de la información.
- Proteger los activos ante desastres provocados por la mano del hombre y de actos hostiles.
- Proteger a la Organización contra situaciones externas como desastres naturales y sabotajes
- En caso de desastre, contar con los planes y políticas de contingencias para lograr una pronta recuperación.
- Contar con los seguros necesarios que cubran las pérdidas económicas en caso de desastre.

Los motivos de los delitos por ordenador normalmente son por:

- Beneficio personal. Obtener un beneficio, ya sea económico, político, social o de poder, dentro de la Organización.
- Beneficios para la Organización. Se considera que al cometer algún delito en otro ordenador se ayudará al desempeño de la Organización en lacual se trabaja, sin evaluar sus repercusiones.
- Síndrome de "Robin Hood" (por beneficiar a otras personas). Se están haciendo copias ilegales por considerar que al infectar a los ordenadores, o bien al alterar la información, se ayudará a otras personas.
- Jugando a jugar.
- Fácil de desfalcar.
- El individuo tiene problemas financieros.
- El Ordenador no tiene sentimientos. El Ordenador es una herramienta que es fácil de desfalcar, y es un reto poder hacerlo.
- El Departamento es deshonesto
- Odio a la Organización (revancha). Se considera que el Departamento o la Organización es deshonesta, ya que no ha proporcionado todos los beneficios a los que se tiene derecho
- Equivocación de ego (deseo de sobresalir en alguna forma).
- Mentalidad turbada. Existen individuos con problemas de personalidad que ven en elaborar un virus un reto y una superación, los cuales llegan a ser tan cínicos que ponen su nombre y dirección e el virus, para lograr ese reconocimiento.

En la actualidad, principalmente en los ordenadores personales, se ha dado otro factor que hay que considerar: el llamado "virus" de los ordenadores, el cual, aunque tiene diferentes intenciones, se encuentra principalmente en paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco.

Se trata de pequeñas subrutinas escondidas en los programas que se activan cuando se cumple alguna condición; por ejemplo, haber obtenido una copia de forma ilegal, y puede ejecutarse en una fecha o situación predeterminada. El virus normalmente es puesto por los diseñadores de algún tipo de programa *("software")* para *"castigar"* a quienes roban o copian sin autorización o bien por alguna actitud de venganza en contra de la Organización. (En la actualidad existen varios productos para detectar virus).

Existen varios tipos de virus, pero casi todos actúan como "Caballos de Troya"; es decir, se encuentran dentro de un programa y actúan con determinada indicación. Un ejemplo es la destrucción de la información de la Compañía USPA & IRA de Forth Worth. Cuando despidieron a un programador en 1985, éste dejó una subrutina que mensualmente destruía la información de las ventas. Este incidente provocó el primer juicio en Estados Unidos de América contra una persona por sabotaje a un Ordenador.

Al auditar los sistemas, se debe tener cuidado que no se tengan copias *"piratas"* o bien que, al conectarse en red con otros ordenadores, no exista la posibilidad de transmisión del virus. También se debe que en ocasiones se toma como pretexto el virus y se producen efectos psicológicos en los usuarios, ya que en el momento de una falla del ordenador o del sistema, lo primero que se piensa es que están infectados, (Bacard, 2002). Se considera que hay cinco factores que han permitido el incremento en los crímenes por ordenador:

- El aumento del número de personas que se encuentran estudiando computación.
- El aumento del número de empleados que tienen acceso a los equipos.
- La facilidad en el uso de los equipos de cómputo.
- El incremento en la concentración del número de aplicaciones y, consecuentemente, de la información.
- El incremento de redes y de facilidades para utilizar los ordenadores en cualquier lugar y tiempo.

Estos cinco factores, aunque son objetivos de todo Centro de Cómputo, también constituyen una posibilidad de uso con fines delictivos. El uso inadecuado del ordenador comienza desde la utilización de tiempo de máquina para usos ajenos al de la Organización, la copia de programas para fines de comercialización sin reportar los derechos de autor, hasta el acceso por vía telefónica a Bases de Datos a fin de modificar la información con fines fraudulentos. Estos delitos pueden ser cometidos por personas que no desean causar un mal.

En la actualidad las compañías cuentan con grandes dispositivos para la seguridad física de los ordenadores, y se tiene la idea que los sistemas no pueden ser violados si no se entra al Centro de Cómputo, olvidando que se pueden usar terminales y sistemas remotos de teleproceso. Se piensa (como en el caso de la seguridad ante incendio y robo), que *"eso no me puede suceder a mí o es poco probable que suceda aquí"*.

Algunos gerentes creen que los ordenadores y sus programas son tan complejos que nadie fuera de su Organización los van a entender y no les van a servir. Pero, en la actualidad, existe un gran número de personas que puede captar y usar la información que contiene un sistema y considerar que hacer esto es como un segundo ingreso. También se ha detectado que el mayor número de fraudes, destrucción de información o uso ilegal de ésta, provienen del personal interno de una Organización. También se debe considerar que gran parte de los fraudes hechos por ordenador o el mal uso de éste son realizados por personal de la misma Organización.

En forma paralela, al aumento de los fraudes hechos a los sistemas computarizados, se han perfeccionado los sistemas de seguridad tanto física lógica; la gran desventaja del aumento en la seguridad lógica es que se requiere consumir un número mayor de recursos de cómputo para lograr tener una idónea seguridad, lo ideal es encontrar un sistema de acceso adecuado al nivel de seguridad requerido por el sistema con el menor costo posible. En los desfalcos por ordenador (desde un punto de vista técnico), hay que tener cuidado con los "Caballos de Troya" que son programas a los que se les encajan rutinas que serán activadas con una señal específica.

IV.2.- Seguridad Lógica y Confidencialidad.

La seguridad lógica se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada de un Ordenador, así como de controlar el mal uso de la información. Estos controles reducen el riesgo de caer en situaciones adversas, según Arkin (2000).

Se puede decir entonces que un inadecuado control de acceso lógico incrementa el potencial de la Organización para perder información, o bien para que ésta sea utilizada en forma inadecuada; así mismo, esto hace que se vea disminuida su defensa ante competidores, el crimen organizado, personal desleal y violaciones accidentales.

La seguridad lógica se encarga de controlar y salvaguardar la información generada por los sistemas, por el *"software"* de desarrollo y por los programas en aplicación; identifica individualmente a cada usuario y sus actividades en el sistema, y restringe el acceso a datos, los programas de uso general, de uso específico, de las redes y terminales. La falta de seguridad lógica o su violación puede traer las siguientes consecuencias ala Organización:

- Cambio de los datos antes o cuando se le da entrada al ordenador.
- Copias de programas y / o información.
- Código oculto en un programa.
- Entrada de virus.

La seguridad lógica puede evitar una afectación de pérdida de registros, y ayuda a conocer el momento en que se produce un cambio o fraude en los sistemas.

El tipo de seguridad puede comenzar desde la simple llave de acceso (contraseña) hasta los sistemas más complicados, pero se debe evaluar que cuanto más complicados sean los dispositivos de seguridad más costosos resultan. Por lo tanto, se debe mantener una adecuada relación de seguridad-costo en los sistemas de información.

Los sistemas de seguridad normalmente no consideran la posibilidad de fraude cometida por los empleados en el desarrollo de sus funciones. La introducción de información confidencial al ordenador puede provocar que ésta esté concentrada en manos de unas cuantas personas, por lo que existe una alta dependencia en caso de pérdida de los registros. El más común de estos delitos se presenta en el momento de la programación, en el cual por medio de ciertos algoritmos se manda borrar un archivo. Por ejemplo, al momento de programar un sistema de nómina se puede incluir una rutina que verifique si se tiene dentro del archivo de empleados el Registro Federal de Contribuyentes del programador.

En caso de existir, continúa el proceso normalmente; si no existe significa que el programador que elaboró el sistema renunció o fue despedido y en ese momento pudo borrar todos los archivos. Esta rutina, aunque es fácil de detectar, puede provocar muchos problemas, en caso de que no se tenga los programas fuente o bien que o se encuentren debidamente documentados. También en el caso de programadores honestos, en ocasiones en forma no intencional, se pueden tener fallas o negligencia en los sistemas. La dependencia de ciertos individuos clave, algunos de los cuales tienen un alto nivel técnico, comúnmente pone a la Organización en manos de unas cuantas personas, las cuales suelen ser las únicas que conocen los sistemas debido a que no los documentan.

Un método eficaz para proteger sistemas de computación es el *"software"* de control de acceso. Dicho de una manera simple, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden al usuario una contraseña antes de permitirle acceso a información confidencial.

Dichos paquetes han sido populares desde hace muchos años en el mundo de los ordenadores grandes, y los principales proveedores ponen a disposición de los clientes alguno de estos paquetes. Sin embargo, los paquetes de control de acceso basados en contraseñas pueden ser eludidos por delincuentes preparados en computación, por lo que no es conveniente depender de esos paquetes por sí solos para tener una adecuada seguridad. El sistema integral de seguridad debe comprender:

- Elementos administrativos.
- Definición de una política de seguridad.
- Organización y división de responsabilidades.

IV.3.- Seguridad Lógica.

Uno de los puntos más importantes a considerar para poder definir la seguridad de un sistema es el grado de actuación que puede tener un usuario dentro de un sistema, ya sea que la información se encuentre en un archivo normal o en una Base de Datos, o bien que posea un miniordenador, o un sistema en red (interna o externa). Para esto se pueden definir los siguientes tipos de usuarios:

- ✓ *Propietario.* Es, como su nombre lo indica, el dueño de la información, el responsable de ésta, y puede realizar cualquier función (consultar, modificar, actualizar, dar instrucciones de entrada a otro usuario). Es responsable de la seguridad lógica, en cuanto puede realizar cualquier acción y puede autorizar a otros usuarios de acuerdo con el nivel que desee darles.

- ✓ *Administrador.* Sólo puede actualizar o modificar el *"software"* con la debida autorización, pero no puede modificar la información. Es responsable de la seguridad lógica y de la integridad de los datos.

- ✓ *Usuario Principal.* Está autorizado por el propietario para hacer modificaciones, cambios, lectura y utilización de los datos, pero no puede dar autorización para que otros usuarios entren.

- ✓ *Usuario de Consulta.* Sólo puede leer la información pero no puede modificarla.

- ✓ *Usuario de Explotación.* Puede leer la información y utilizarla para explotación de la misma, principalmente para hacer reportes de diferente índole, los cuales, por ejemplo, pueden ser contables o estadísticos.

✓ *Usuario de Auditoria.* Puede utilizar la información y rastrearla dentro del sistema para fines de auditoria.

Los usuarios pueden ser múltiples y pueden ser el resultado de la combinación de los antes señalados. Se recomienda que exista sólo un usuario propietario, y que el administrador sea una persona designada por la Gerencia de Informática, (Baker, 2000).

Para conservar la integridad, confidencialidad y disponibilidad de los sistemas de información se debe tomar en cuenta lo siguiente:

- La *Integridad* es responsabilidad de los individuos autorizados para modificar datos o programas (usuario administrador) o de los usuarios a los que se otorgan accesos a aplicaciones de sistema o funciones fuera de sus responsabilidades normales de trabajo (usuario responsable y principal).

- La *Confidencialidad* es responsabilidad de los individuos autorizados para consultar (usuario de consulta) o para bajar archivos importantes para microordenadores (usuario de explotación).

- La *Disponibilidad* es responsabilidad de individuos autorizados para alterar los parámetros de control de acceso al sistema operativo, al sistema manejador de Bases de Datos, al monitoreo de teleproceso o al "software" de telecomunicaciones (usuario administrados).

El control implantado para minimizar estos riesgos debe considerar los siguientes factores:

- El valor de los datos siendo procesados.
- La probabilidad de que ocurra un acceso no autorizado.
- Las consecuencias de la Organización si ocurre un acceso no autorizado.
- El riesgo y repercusiones en caso de que un usuario no autorizado utilice la información.

La seguridad lógica abarca las siguientes áreas:

- Rutas de acceso.
- Claves de acceso.
- *Software* de control de acceso.
- Encriptamiento.

IV. 3.1. Rutas de Acceso.

El acceso a la computadora no significa tener una entrada sin restricciones. Limitar el acceso sólo a los niveles apropiados puede proporcionar una mayor seguridad. El objetivo de la seguridad de los sistemas de información es controlar las operaciones y su ambiente mediante el monitoreo del acceso a la información y a los programas para poder darle un seguimiento y determinar la causa probable de desviaciones, (Barriuso, 1996). Por ello es conveniente al utilizar algún tipo de *"software"* dentro de un sistema, contar con una ruta de acceso.

Cada uno de los sistemas de información tiene una ruta de acceso, la cual puede definirse como la trayectoria seguida en el momento de acceso al sistema.

Como se ha señalado, un usuario puede pasar por uno o múltiples niveles de seguridad antes de obtener el acceso a los programas y datos. Los tipos de restricciones son:

- Sólo lectura.
- Sólo consulta.
- Lectura y consulta.
- Lectura y escritura, para crear, actualizar, borrar, ejecutar o copiar.

El esquema identifica a los usuarios del sistema, los tipos de dispositivos por los cuales es posible acceder al sistema, el *"software"* usado para el acceso al sistema, los recursos que pueden ser accedidos y los sistemas donde residen estos recursos. Los sistemas pueden ser en línea, fuera de línea, en *"batch"*, y rutas de telecomunicación.

El esquema de las rutas de acceso sirve para identificar todos los puntos de control que pueden ser usados para proteger los datos en el sistema. El auditor debe conocer las rutas de acceso para la evaluación de los puntos de control apropiados.

IV.3.2.- Claves de Acceso.

Un área importante en la seguridad lógica es el control de las claves de acceso de los usuarios, (Bernal, 1997). Existen diferentes métodos de identificación para el usuario:

- Un código o contraseña.
- Una credencial con banda magnética.
- Algo específico del usuario (características propias).

La identificación es definida como el proceso de distinción de un usuario a otros. La identificación de entrada proporcionará un reconocimiento individual; cada usuario debe tener una identificación de entrada única que debe ser reconocida por el sistema.

Contraseña, código o llaves de acceso. La identificación de los individuos es usualmente conocida y está asociada con un *"password"* o clave de acceso. Las claves de acceso pueden ser usadas para controlar el acceso a la computadora, a sus recursos, así como definir nivel de acceso o funciones específicas.

Las llaves de acceso deben tener las siguientes características:

- El sistema debe verificar primero que el usuario tenga una llave de acceso válida.
- La llave de acceso debe ser de una longitud adecuada para ser un secreto.
- La llave de acceso no debe ser desplegada cuando es tecleada.
- Las llaves de acceso deben ser encriptadas, ya que esto reduce el riesgo de que alguien obtenga la llave de acceso de otras personas.
- Las llaves de acceso deben de prohibir el uso de nombres, palabras o cadenas de caracteres difíciles de retener, además el *"password"* no debe ser cambiado por un valor pasado. Se recomienda la combinación de caracteres alfabéticos y numéricos. No debe ser particularmente identificable con el usuario, como su nombre, apellido o fecha de nacimiento.

Credenciales con banda magnética. La banda magnética de las credenciales es frecuentemente usada para la entrada del sistema. Esta credencial es como una bancaria, pero se recomienda que tenga fotografía o firma.

La ventaja más importante de la credencial es prevenir la entrada de impostores al sistema. Una credencial ordinaria es fácil de falsificar, por lo que se debe elaborar de una manera especial, que no permita que sea reproducida.

Validación por características. Es un método para la identificación del usuario, que es implantado con tecnología biométrica. Consiste en la verificación y reconocimiento de la identidad de las personas, basándose en características propias. Algunos de los dispositivos biométricos son:

- ✓ Las huellas dactilares.
- ✓ La retina.
- ✓ La geometría de la mano.
- ✓ La firma.
- ✓ La voz.

IV.3.3.- "Software" de Control de Acceso.

Éste puede ser definido como el *"software"* diseñado para permitir el manejo y control del acceso a los siguientes recursos:

- Programas de librerías.
- Archivos de datos.
- *"Jobs"*.
- Programas en aplicación.
- Módulos de funciones.
- Utilerías.
- Diccionario de datos.
- Archivos.
- Programas.
- Comunicación.

Controla el acceso a la información, grabando e investigando los eventos realizados y el acceso a los recursos, por medio de la identificación del usuario, (Caballero, 1996).

El *"software"* de control de acceso, tiene las siguientes funciones:

- o Definición de usuarios.
- o Definición de las funciones del usuario después de acceder al sistema.
- o Establecimiento de auditoria a través del uso del sistema.

El *"software"* de seguridad protege a los recursos mediante la identificación de los usuarios autorizados con las llaves de acceso, que son archivadas y guardadas por este *"software"*.

Esto puede ser efectuado a través de la creación de archivos o tablas de seguridad. Los paquetes de seguridad frecuentemente incluyen facilidades para encriptar estas tablas o archivos.

A cada usuario se le debe asignar un alcance en el acceso y por cada recurso un grado de protección; para que los recursos puedan ser protegidos de un acceso no autorizado.

Algunos paquetes de seguridad pueden ser usados para restringir el acceso a programas, librerías y archivos de datos; otros pueden además limitar el uso de terminales o restringir el acceso a bases de datos, y existen otros más para confirmar y evaluar la autorización de la terminal para utilizar determinada información. Éstos pueden variar en el nivel de la seguridad brindada o los archivos de datos. La seguridad puede estar basada en el tipo de acceso: usuarios autorizados para agregar registros a un archivo o los que únicamente leen registros.

La mayor ventaja del *"software"* de seguridad es la capacidad para proteger los recursos de accesos no autorizados, incluyendo los siguientes:

- Procesos en espera de modificación por un programa de aplicación.
- Accesos por los editores en línea.
- Accesos por utilerías de *"software"*.
- Accesos a archivos de las bases de datos, a través de un manejador de base de datos (DBMS).
- Acceso de terminales o estaciones no autorizadas.

Estos paquetes pueden restringir el acceso a los recursos (archivos de datos), reduciendo así el riesgo de los accesos no autorizados.

En el caso de terminales de compra de boletos de pronósticos, se puede restringir la entrada a terminales no autorizadas o en tiempo no autorizado.

Otra característica de estos paquetes es que se pueden detectar las violaciones de seguridad, tomando las siguientes medidas:

- Terminaciones de procesos.
- Forzar a las terminales a apagarse.
- Desplegar mensajes de error.
- Escribir los registros para la auditoria.

La bitácora de auditoria es seleccionada mediante la implementación.

La bitácora puede consistir en registrar los accesos no exitosos, solo los intelectos, un registro de todos los accesos válidos y los recursos protegidos.

Algunos paquetes contienen datos específicos para ser incluidos en la bitácora de auditoria.

Cada bitácora debe incluir la identificación del usuario; si el acceso es exitoso, deben consignarse los recursos accedidos, día, hora, terminal y un dato específico de lo que fue modificado durante el acceso; si el acceder no fue exitoso la mayor información posible sobre día, hora, terminal y claves de intento usadas.

IV.3.4.- Otros Tipos de "Software" de Control de Acceso.

Algunos tipos de software son diseñados con características que pueden ser usadas para proveerles seguridad. Sin embargo, es preferible usar un *"software"* de control de acceso para asegurar el ambiente total y completar las características de seguridad con un software específico, (Coelli, 2002).

Como existen diferentes tipos de *"software"*, se explicarán las características de seguridad de los siguientes:

- Sistemas operativos.
- Manejadores de base de datos.
- Software de consolas o terminales maestras.
- Software de librerías.
- Software de utilerías.
- Telecomunicaciones.

A) Sistemas Operativos.

Se trata de una serie de programas que se encuentran dentro de los sistemas operativos, los cuales manejan los recursos de las computadoras y sirven como interfase entre el *"software"* de aplicaciones y el *"hardware"*.

Estos programas proporcionan seguridad ya que, internamente, dentro de los sistemas operativos manejan y controlan la ejecución de programas de aplicación y proveen los servicios que estos programas requieren, dependiendo del usuario y del sistema que se esté trabajando. Cada servicio debe incluir un calendario de trabajo (*"Job Schedule"*), manejador de equipos periféricos, un contador de trabajo y un compilador de programas, pruebas y *"debugs"* (depuraciones). El grado de protección sobre estos servicios depende de los sistemas operativos.

Los elementos de seguridad de los sistemas operativos incluyen los siguientes:

- Control de salidas de los programas al modificarse códigos. Éstos usualmente pueden acceder a los elementos más importantes del sistema, y sus actividades deben ser monitoreadas.
- Los sistemas operativos usan claves de acceso (*"password"*, ID) para prevenir usuarios no autorizados a funciones y utilerías del sistema operativo. Muchas veces, estas claves de acceso están definidas en una tabla del sistema que es activada cuando un sistema es utilizado. Las claves de acceso deben ser cambiadas inmediatamente por las nuevas claves de acceso.
- Algunos sistemas operativos proveen una característica que puede limitar el número de accesos no autorizados y autorizar usuarios a los recursos protegidos, si este número es excedido, el usuario no autorizado es prevenido para el nuevo acceso a estos recursos.
- Los sistemas operativos permiten una instalación para la implementación opcional de características de seguridad cuando es sistema es instalado. Algunos sistemas operativos contienen sus propias características de seguridad y muchas veces éstas no son adecuadas; en este caso es aconsejable integrar al sistema operativo un *"software"* de seguridad para proteger los recursos. El valor de estos es un factor determinante cuando se decide que tanta protección es necesaria.
- Los sistemas operativos tienen un completo control sobre las actividades de todas las aplicaciones que estás corriendo en el sistema. Si un usuario no autorizado puede acceder a los recursos del sistema operativo, puede hacer modificaciones que alteren el proceso normal del flujo del sistema. El sistema operativo tiene autoridad para dar facilidades de seguridad y para acceder a recursos confidenciales. Esto implica que en algunas ocasiones se requerirá del uso de algún producto de seguridad adicional. El *"software"* de funciones de control del sistema operativo debe proveer una bitácora de auditoria.
- Tanto el administrador del sistema o de seguridad de datos establece sus privilegios a través del sistema operativo. Individualmente, con estos privilegios tienen completo control sobre el sistema operativo y su ambiente; ellos pueden otorgar la autoridad para modificar usuarios y acceder a secciones, alterar la generación de procedimientos del sistema y modificar las prioridades de trabajo (*"jobs"*) que corren dentro del control del sistema.

Debe existir una bitácora de las actividades del administrador del sistema o del administrador de la seguridad de datos.

- Los sistemas operativos permiten la definición de consolas o terminales maestras desde las cuales los operadores puede introducir comandos al sistema operativo. Las consolas no requieren una señal en proceso para la emisión de comandos. Por lo tanto, el acceso, a áreas físicas en donde están las consolas debe ser restringido. Además, las características del sistema que permiten a una terminal ser asignada con el estatus de consola deben ser guardadas a prueba de accesos no autorizados.

B) *"Software"* Manejador de Base de Datos.

Es un *"software"* cuya finalidad es la de controlar, organizar y manipular los datos. Provee múltiples caminos para acceder a los datos, en una base de datos. Maneja la integridad de datos entre operaciones, funciones y tareas de la organización.

Cuando un usuario inicialmente requiere del uso de sistemas de administración de bases de datos *("Data Base Management System", DBMS)* se establece un identificador para el usuario y la sesión. Inmediatamente, el usuario puede ser identificado por el ID-terminal, y por una aplicación o función.

En espera del modo de modificaciones, el usuario podrá ser identificado por el trabajo (*"job"*), por la aplicación o por la función.

El identificador del usuario será usado para rastrear todos loa accesos a los archivos de datos a través del administrador de la base de datos (DBMS).

Las características de seguridad del software DBMS pueden ser usadas para restringir el acceso a un usuario específico, a un cierto archivo o a vistas lógicas, los accesos a procedimientos, funciones o *"software"* en aplicaciones limitado a usuarios autorizados con el propósito de ejecutar sus tareas asignadas. Las vistas de datos lógicos están colocadas en archivos para usuarios particulares, funciones o aplicaciones, y puede ser representado todo o parte del archivo de datos físicos o una combinación de campos de múltiples archivos de datos físicos. Estas características son usadas para controlar funciones únicas en el administrador de la base de datos (DBMS).

Las utilerías de la base de datos proveen funciones de mantenimiento, como respaldos y restauración de la base de datos, reorganización de datos, reportes estadísticos de la base de datos y sus relaciones. Ésos pueden ser usados además para adicionar o borrar datos y proveer seguridad.

El diccionario de datos (DD) es un *"software"* que guía y provee un método para documentar elementos de la base de datos, así como un método de seguridad de datos en un administrador de base de datos (DBMS).

Todas las modificaciones al director de datos (DD) deben producir una bitácora de auditoria, como un registro automático de todos los cambios y un medio de recuperación después de alguna interrupción que hubiese ocurrido.

C) *"Software"* de Consolas o Terminales Maestras.

El *"software"* de consolas o terminales maestras puede ser definido como varios programas del sistema operativo que proveen soporte y servicio para que las terminales en linea accedan a los programas en aplicación.

Las consolas incluyen funciones de seguridad para restringir el acceso a los datos, vía programas en aplicación.

Estas funciones frecuentemente están basadas en una serie de tablas que definen a los usuarios autorizados, así como los recursos y programas en aplicación que ellos pueden acceder. Generalmente las consolas pueden sólo limitar al acceso al usuario para entrar a un programa en aplicación, no para el uso de funciones especificas de un programa.

La mayor parte de las consolas mantienen un registro de uso de llaves de acceso (*"password"*) diario válidas o no válidas.

D) *"Software"* de Librerías.

El *"software"* de librerías consta de datos y programas específicos escritos para ejecutar una función en la organización.

Los programas en aplicación (librerías) pueden ser guardados en archivos en el sistema y acceder a estos programas puede ser controlado por medio del *"software"* (*"software"* de control de acceso general) usado para controlar el acceso a estos archivos.

El *"software"* de manejo de librerías puede ser usado para mantener y proteger los recursos de programas de librerías, la ejecución de *"jobs"*, y en algunas instancias, los archivos de datos pueden ser utilizados por éstas.

Estas librerías deben ser soportadas por un adecuado control de cambios y procedimientos de documentación.

Una importante función del *"software"* controlador de librerías es controlar y describir los cambios de programas en una bitácora. El *"software"* de librerías provee diferentes niveles de seguridad, los cuales se reflejan en las bitácoras de auditoria.

Los controles de cambios de emergencia deben estar en algún lugar debido a la naturaleza de estos cambios (frecuentemente son realizados fuera de horas de trabajo normal, son cortos, no se comunican):

- Accesos de emergencia. Pueden ser concedidos con el propósito de resolver el problema, y ser inmediatamente revocados después de que el problema es resuelto.
- Todas las acciones realizadas durante la emergencia deberán ser automáticamente registradas.

Cuando se instala el software de librerías se definen las librerías y sus respectivos niveles de protección.

Los tipos de acceso a la librería pueden ser registrados durante la instalación. Por ejemplo, un programador deberá ser autorizado para leer o modificar un programa.

E) *"Software"* de Utilerías.

Existen dos tipos de *"software"* de utilerías. El primero es usado en los sistemas de desarrollo para proveer productividad. El desarrollo de programas y los editores en línea son los ejemplos de este tipo de *"software"*. El segundo es usado para asistir en el manejo de operaciones del Ordenador. Monitoreos, calendarios de trabajo, sistema manejador de disco y cinta son ejemplos de este tipo de *"software"*.

El *"software"* de utilerías tiene privilegios para acceder todo el tiempo, algún tiempo o nunca. Los accesos privilegiados se otorgan en programadores o a usuarios que ejecutan funciones que sobrepasan la seguridad normal.

Entre los ejemplos de utilerías de *"software"* están:

- ✓ Utilerías de monitores.
- ✓ Sistemas manejadores de cintas.
- ✓ Sistemas manejadores de disco.

- ✓ Calendarios de *"jobs"*.
- ✓ Editores de línea.
- ✓ *"Debugers"*.
- ✓ Verificador de virus.
- ✓ *"Software"* de telecomunicaciones.

Ciertos tipos de *"software"* de telecomunicaciones pueden restringir el acceso a las redes y a aplicaciones específicas localizadas en la red.

El *"software"* de telecomunicaciones provee la interfase entre las terminales y las redes y tiene la capacidad para:

- Controlar la invocación de los programas de aplicación.
- Verificar que todas las transacciones estén completas y sean correctamente transmitidas.
- Restringir a los usuarios para actuar en funciones seleccionadas.
- Restringir al acceso al sistema a ciertos individuos.

IV.4.- Riesgos y Controles a Auditar.

Los controles de *"software"* de seguridad general y de *"software"* específico pueden ser implantados para minimizar el riesgo de la seguridad lógica, (Calle, 1997).

Controles del *"software"* de seguridad general. Los controles del *"software"* de seguridad general aplican para todos los tipos de *"software"* y recursos relacionados y sirven para:

- El control de acceso a programas y a la información.
- Vigilar los cambios realizados.
- Las bitácoras de auditoria.
- Control de acceso a programas y datos. Este control de acceso se refiere a la manera en que cada *"software"* del sistema tiene acceso a los datos, programas y funciones. Los controles son usualmente a través del ID (identificador) o del *"password"* para identificar a usuarios no autorizados y para controlar el acceso inicial al *"software"*.
- Cambios realizados. Deben ser probados y revisados para ser autorizados, y una vez autorizados se asignan a los programas en aplicación y datos.

Dependiendo de la aplicación, el ambiente y el potencial del efecto de los cambios, éste puede ser muy informal o extremadamente rígido. Los procedimientos a seguir para los cambios realizados pueden ser los siguientes:

- Diseños y código de modificaciones.
- Coordinación con otros cambios.
- Asignación de responsabilidades.
- Revisión de estándares y aprobación.
- Requerimientos mínimos de prueba.
- Procedimientos del respaldo en el evento de interrupción.

La bitácora de auditoria debe registrar cambios en el *"software"* antes de la implementación. Los procedimientos de cambios de *"software"* deben además incluir notificaciones escritas para el departamento apropiado de cada cambio. Los cambios realizados deben incluir independientemente una fase de pruebas realizadas por un grupo fuera del ambiente de desarrollo.

- Bitácoras de Auditoria. Las bitácoras de auditoria son usadas para monitorear los accesos permitidos y negados. *El "software"* debe contener una bitácora de auditoría de uso de las funciones que el *"software"* ejecuta, particularmente si cambian las funciones o se modifican datos. Esta bitácora de auditoria posiblemente sea mantenida en un archivo separado, y puede ser manejada por las actividades del sistema, o tal vez sea una parte del registro. El tipo de bitácoras de auditoría varía gradualmente de acuerdo al *"software"* y al vendedor; por ejemplo, un *"software"* puede guardar antes y después imágenes de los cambios, mientras que otros solamente tienen una técnica de recuperación que puede ser usada para seguridad en casos necesarios.

Las bitácoras de auditoría generalmente están relacionadas con el sistema operativo o con el *"software"* de control de acceso. Estas bitácoras de auditoría registran las actividades y opcionalmente muestran el registro de los cambios hechos en el archivo o programas. Son importantes para el seguimiento de los cambios.

Controles de *"software"* especifico. A continuación se presentan algunos de los controles usados por los diferentes tipos de *"software"* especifico:

- El acceso al sistema debe ser restringido para individuos no autorizados.
- Se debe controlar el acceso a los procesos y a las aplicaciones permitiendo a los usuarios autorizados ejecutar sus obligaciones asignadas y evitando que personas no autorizadas logren el acceso.
- Las tablas de acceso o descripciones deberán ser establecidas de manera que se restrinja a los usuarios ejecutar funciones incompatibles o más allá de sus responsabilidades.
- Se deberá contar con procedimientos para que los programadores de aplicaciones tengan prohibido realizar cambios no autorizados a los programas.
- Se limitará tanto a usuarios como a programadores de aplicaciones a un tipo específico de acceso de datos (por ejemplo: lectura y modificación).
- Para asegurar las rutas de acceso deberá restringirse el acceso a secciones o tablas de seguridad, mismas que deberán ser encriptadas.
- Las bitácoras de auditoria deberán ser protegidas de modificaciones no autorizadas.

Deberán restringirse las modificaciones o cambios al *"software"* de control de acceso, y éstos deberán ser realizados de acuerdo a procedimientos autorizados:

1.- *"Software"* de sistemas operativos. Entre los controles se incluyen los siguientes:

- Los *"password"* e identificadores deberán ser confidenciales. Los usuarios no autorizados que logran acceder al sistema pueden causar modificaciones no autorizadas.
- El acceso a *"software"* de sistema operativo deberá ser restringido.
- Los administradores de la seguridad deberán ser los únicos con autoridad para modificar funciones del sistema, incluyendo procedimientos y tablas de usuarios.
- El acceder a utilerías del sistema operativo será restringido.
- Las instalaciones de sistemas y las reinstalaciones deben ser monitoreadas porque la realización no autorizada puede resultar inválida.
- El uso de todas las funciones del *"software"* (editores de línea, consolas) es restringido a individuos autorizados.
- Deberán revisarse las bitácoras de auditoria para determinar si ocurre un acceso no autorizado o si se realizan modificaciones.

2.- *"Software"* manejador de base de datos. Los controles incluyen lo siguiente:

- ✓ El acceso a los archivos de datos deberá ser restringido en una vista de datos lógica, a nivel de tipo de campo. La seguridad en el campo será dada de acuerdo al contenido del campo (validación de campos).
- ✓ Deberá controlarse al acceso al diccionario de datos.

- ✓ La Base de Datos debe ser segura y se usarán las facilidades de control de acceso construidas dentro del *"software"*, DSMS.
- ✓ La bitácora de auditoria debe reportar los accesos al diccionario de datos.
- ✓ Las modificaciones de capacidades desde el DBMS para las bases de datos deberán limitarse al personal apropiado.

3.-*"Software"* de consolas o terminales maestras. Estos controles incluyen lo siguiente:

- Los cambios realizados al *"software"* de consolas o terminales maestras deberán ser protegidos y controlados.

4.- *"Software"* de librerias. Los controles incluyen lo siguiente:

- El *"software"* de librerías mantiene una bitácora de auditoria de todas las actividades realizadas. La información provista en la bitácora incluye el nombre del programa, el número de la versión, los cambios específicos realizados, la fecha de mantenimiento y la identificación del programador.
- El *"software"* de librerías tiene la facilidad de comparar dos versiones de programas en código fuente y reportar las diferencias.
- Debe limitarse al acceso a programas o datos almacenados por el "software" de librerías.
- Deberá impedirse al acceso a *"password"* o códigos de autorización a individuos no autorizados.
- Los cambios realizados al *"software"* de librerías tendrán que ser protegidos y controlados.
- Las versiones correctas de los programas de producción deben corresponder a los programas objeto.

5.- *"Software"* de utilerías. Los controles incluyen lo siguiente:

- Deberá restringirse el acceso a archivos de utilerías.
- Algunas utilerías establecen niveles de utilización por cada función y verifican cada nivel de autorización del usuario antes de darle acceso, utilizando *"password"* para proveer accesos no autorizados.
- El *"software"* de utilerías genera una bitácora de auditoria de usos y actividades. Algunas proveen bitácoras detalladas de actividades con datos protegidos, librerías y otros recursos. Estas bitácoras de auditoria proveen información de cada identificador (ID), fecha y hora de acceso, recursos accedidos y tipo de acceso.
- Esta bitácora sirve como un registro de eventos, incluyendo violaciones a la seguridad y accesos no autorizados. Cada paquete de *"software"* puede tener diferentes capacidades de control.
- Tomar precauciones para asegurar la manipulación de datos (copiar, borrar, etcétera), los protege de un uso no autorizado.
- Asegurar que únicamente personal autorizado tenga acceso a correr aplicaciones.

- Las utilerías no deben ser mantenidas en el ambiente de producción y se debe asegurar que únicamente usuarios autorizados tengan acceso a ellas.
- Las bitácoras de auditoria producidas por utilerías deben ser cuidadosamente revisadas para identificar alguna violación a la seguridad.

6.- *"Software"* de telecomunicaciones. Los controles incluyen lo siguiente:

Controlar el acceso a datos sensibles y recursos de la red de la siguiente forma:

- Verificación de *"login"* de aplicaciones.
- Control de las conexiones entre sistemas de telecomunicaciones y terminales.
- Restricción al uso de aplicaciones de la red.
- Protección de datos sensibles durante la transmisión, terminando la sesión automáticamente.

  - Los comandos del operador que pueden dar *"shoutdown"* a los componentes de la red sólo pueden ser usados por usuarios autorizados.
  - El acceso diario al sistema debe ser monitoreado y protegido.
  - Asegurar que los datos no sean accedidos o modificados por un usuario no autorizado, ya sea durante la transmisión o mientras está en almacenamiento temporal.

IV.4.1.- Consideraciones al Auditar.

Cuando se realiza una revisión de seguridad lógica, el auditor interno deberá evaluar y probar los siguientes tres controles implantados para minimizar riesgos:

- Control de acceso a programas y a la información.
- Control de cambios.
- Bitácoras de auditoria.

La evaluación de todos los tipos de *"software"* deberá asegurar que los siguientes objetivos sean cumplidos:

- El acceso a funciones, datos y programas asociados con el *"software"* debe estar restringido a individuos autorizados y debe ser consistente con documentos esperados.

- Todos los cambios del *"software"* deben ser realizados de acuerdo con el manejo del plan de trabajo y con la autorización del usuario.
- Se debe mantener una bitácora de auditoría de todas las actividades significativas.

La auditoría de seguridad lógica puede ser realizada de diferentes maneras. La auditoría puede enfocarse en áreas de seguridad que son aplicables a todo tipo de *"software"* y pueden cubrir la instalación, el mantenimiento y la utilización del *"software"*.

También debe tomarse en cuenta las características de seguridad del *"software"*, incluyendo el control de acceso, la identificación del usuario y el proceso de autenticidad del usuario, ejecutado por el *"software"*. Entre las consideraciones específicas al auditar están:

- ✓ *"Software"* de control de acceso.
- ✓ *"Software"* de telecomunicaciones.
- ✓ *"Software"* manejador de librerías.
- ✓ *"Software"* manejador de Bases de Datos.
- ✓ *"Software"* de utilerías.
- ✓ *"Software"* de Sistema Operativo.

Durante el ciclo de vida del *"software"* deben ser evaluadas su instalación, mantenimiento y operación. Se debe utilizar la auditoría para asegurar que algún cambio hecho al *"software"* no comprometa la integridad, confidencialidad o aprovechamiento de los datos o recursos del sistema. El *"software"* de auditoría especializado puede ser usado para revisar todos los cambios y asegurarse que son ejecutados de acuerdo con los procedimientos aprobados por la Gerencia.

Instalación y mantenimiento. Es la primer fase del ciclo de vida del *"software"*, en el cual el auditor debe revisar lo siguiente:

- Procedimientos para nuevas pruebas o modificaciones al *"software"*, incluyendo al personal responsable, ejecución de pruebas, respaldo de *"software"* existente, pruebas de funciones, documentación de cambios, notificación de cambios, revisión y redención de pruebas de salida y aprobación de prioridades para la implantación.
- Procedimientos para iniciación, documentación, pruebas y aprobación de modificaciones al *"software"*.
- Procedimientos usados para ejecutar *"software"* y mantenimiento del diccionario de datos para un mayor grado de modificación.
- Procedimiento de emergencia usados para dar solución a un problema específico de *"software"*.

- Mantenimiento y contenido de las bitácoras de auditoría de todos los DBMS y modificaciones del diccionario de datos.
- Bitácoras a los parámetros del "software" y de las sentencias del lenguaje de aplicaciones en ejecución.
- Acceso a librerías de programas.

Operación. En la segunda fase del ciclo de vida del *"software"* deberán revisarse:

- Controles de acceso para los programas, librerías, parámetros, secciones o archivos de *"software"* asociados.
- Procedimientos diseñados para asegurar que el sistema no es instalado (carga inicial del programa) sin el *"software"* original, creando así un procedimiento de seguridad.
- Disponibilidad y control de acceso a los comandos que pueden ser usados para desactivar el *"software"*.
- Áreas de responsabilidad para el control del *"software"*, operación y consistencia de capacidad de acceso.
- Horas durante las cuales el *"software"* está disponible.
- Procedimientos para la iniciación y terminación del uso del *"software"*.
- Control de acceso sobre consolas y terminales maestras.
- Procedimientos para registrar terminación anormal o errores, los cuales pueden indicar problemas en la integridad del *"software"* y documentar los resultados en programas de seguridad.
- Controles de acceso sobre escritura de programas y lenguajes de librerías y de aplicaciones en ejecución.
- Bitácoras de auditoría sobre las actividades del *"software"*.
- Dependencia de otro *"software"* para continuar la operación, operaciones automatizadas o dependencia del calendario de actividades.

***"Software"* de control de acceso.** Entre las consideraciones de auditoría para el *"software"* de control de acceso están:

- Diseño y administración.
- Procedimiento de identificación del usuario.
- Procedimientos de autentificación del usuario.
- Recursos para controlar el acceso.
- Reportes y vigilancia del *"software"* de control de acceso reportando y vigilando.

El *"software"* de control de acceso usualmente provee utilerías que pueden ser usadas en la ejecución de una auditoría. Los eventos pueden ser registrados en un archivo de auditoría (cambios en el sistema, así como la ocurrencia de otras numerosas actividades: *"login"*, archivos de acceso, recursos de acceso, violaciones y cambios de acceso). Los reporteadores y otras utilerías pueden ser usadas para presentar esta información continuamente.

- Diseño y administración. En estos aspectos los auditores internos deben revisar lo siguiente:
  - Localización de archivos de seguridad, tablas para asegurar que los archivos del *"software"* de control de acceso están protegidos.
  - Uso de recursos o controles de acceso a nivel del usuario para asegurar que el *"software"* de control de acceso protege datos y recursos en un nivel correcto.
  - Archivos de seguridad o encriptación de tablas usadas para prohibir la vista de tablas individuales.
  - Limitaciones de acceso para archivos de seguridad que contienen descripciones y contraseñas.
  - Limitaciones de acceso a archivos de seguridad a través de la administración de comando de seguridad en línea o utilerías.
  - Los usuarios encargados de la administración de la seguridad pueden tener gran capacidad para cierto *"software"*.
  - Métodos y limitaciones sobre archivos de seguridad o modificación de tablas.
  - Responsabilidades del usuario para la administración de la seguridad, particularmente en un ambiente descentralizado, para asegurar que las capacidades definidas son consistentes con las responsabilidades.
  - Definición de parámetros de seguridad, como los recursos definidos, reglas de contraseña(s), *"default"* de niveles de acceso y opciones de *"login"* con aprobación de la Gerencia, considerando pruebas de protección para acceder recursos protegidos.

- Procedimientos de identificación del usuario. Los auditores deberán revisar y aprobar los métodos usados para definir usuarios para el *"software"*. Las siguientes situaciones deberán ser revisadas por un apropiado nivel de dirección:
  - Las identificaciones del usuario para corroborar que sean individuales y no compartidas.
  - Probar la revocación de usuarios inactivos.
  - El despliegue de la última fecha y hora en que algún ID específico fue usado. Esta información podrá ayudar para identificar actividades ilícitas.

- Revocación o desconexión de identificaciones del usuario siguiendo un número específico de acceso inválido. Este control puede también limitar actividades ilícitas.
- El uso de comienzo y fin de fechas para ID de usuario de empleados contratados.
- El uso de grupos de usuarios para el recurso de acceso a los archivos. Los usuarios deberán ser asignados a los grupos apropiados.

- Procedimientos de autentificación del usuario. Los auditores internos deberán revisar lo siguiente:

  - Deberá ser evaluado el uso de contraseñas o información personal durante la sesión.
  - Deberá ser identificada la disponibilidad de automatizar funciones una vez identificado el usuario, así como la autenticación de procedimientos.
  - Deberá ser identificado el uso de contraseñas por otro personal que no sean los usuarios autorizados.
  - Los procedimientos para el uso de contraseñas para asegurarse que éste está protegido cuando es usado por el usuario.
  - La máscara de la contraseña para asegurarse que el área donde los caracteres son tecleados no se desplieguen.
  - La sintaxis de la contraseña. Algún *"software"* de control de acceso puede restringir el uso de ciertas palabras o cadenas de caracteres.
  - El mantenimiento de la historia de la contraseña. Éste puede ser usado para prevenir a usuarios que reutilizan una contraseña por un período específico.
  - Procedimientos para suplir identificaciones de usuarios y contraseñas por procesos *"batch"*.

- Los recursos para controlar e acceso. Los auditores internos deberán revisar lo siguiente:

- ✓ Posibles niveles de acceso.
- ✓ Niveles de acceso por *"default"*, particularmente para usuarios o *"jobs"* que no tienen un ID de usuario.
- ✓ El acceso del usuario a archivos de seguridad.
- ✓ Que la seguridad sea implantada en el nivel correcto.
- ✓ Procedimientos para asegurar la protección automática.
- ✓ Procedimientos para la protección de recursos.
- ✓ Uso de rutas rápidas o funciones aceleradas a través de controles.
- ✓ Controles de acceso sobre aplicaciones locales o remotas.

- ✓ Restricciones de acceso sobre recursos críticos del sistema, tales como sistemas, programas y aplicaciones en ejecución, librerías del lenguaje, catálogos del sistema y directorios, diccionarios de datos, *"logs"* y archivos de contraseñas, tablas de definición de privilegios, algoritmos de encriptación y tablas de datos.

    - Reportes y vigilancia del *"software"* de control de accesos. EL auditor interno deberá revisar:

        - o *"Login"*, identificación del acceso autorizado al sistema y el uso de recursos.
        - o Las identificaciones de acceso no autorizado.
        - o La identificación de archivos de seguridad, mantenimiento a tabla y el uso de comando sensibles.
        - o El *"login"* de usuarios privilegiados y sus actividades.
        - o Las restricciones de acceso a archivos de *"log"* del sistema. Estos archivos frecuentemente contienen las bitácoras de auditoría del control de acceso.
        - o Sistema Operativo o *"software"* de control de acceso existente
        - o Las violaciones a la seguridad.
        - o Los archivos de seguridad y la generación de reportes de las actividades del usuario para asegurar que los propietarios de datos y recursos son notificados de los eventos de seguridad en un periodo determinado.

Sistemas operativos. El auditor deberá revisar, evaluar y probar el uso y procedimientos que gobiernan programas, usuarios y funciones del sistema operativo, especialmente los siguientes:

- ❑ Las facilidades del Sistema Operativo, como son la supervisión y privilegios para programas y usuarios.
- ❑ Controles de acceso sobre tablas que definen privilegios de usuarios, programas y funciones.
- ❑ Controles de acceso sobre consolas o terminales maestras y privilegios asociados.
- ❑ Bitácoras de auditoría.
- ❑ Posibilidade y uso del control de acceso sobre los *"default"* de inicio de ID de usuarios y contraseñas.
- ❑ Comandos de *"software"* o funciones que son consideradas importante, como mantenimiento de seguridad al archivo de descripciones.
- ❑ Diagnóstico de utilerías del Sistema Operativo que pueden ser usados para leer o almacenar áreas que contienen información importante.

***"Software"* del sistema manejador de Bases de Datos.** En relación con las funciones del *"software"* que restringen el acceso a datos y recursos , y los procedimientos que gobiernan el uso de estas funciones, el auditor deberá revisar, evaluar y probar lo siguiente:

- Procedimientos usados por el *"software"* de control de acceso para restringir el acceso a la Base de Datos y al direccionamiento de datos.
- El diseño de una restricción de acceso en los archivos por niveles, incluyendo restricciones sobre archivos físicos y lógicos en el DBMS y en el diccionario de datos.
- Seguridad de campos, uso de secciones de usuarios y contraseñas y restricciones de acceso.
- Si el *"software"* ejecuta la función de identificación del usuario y procedimientos de autentificación.
- Comandos y funciones del diccionario de datos (utilerías del Adminisrador de la Base de Datos, comandos para modificar DSMS, archivo o definiciones de archivo).
- Accesos de los programadores, acceso a DBMS y comandos o funciones del directorio de datos.
- Bitácoras de auditoría.
- El *"software"* de desarrollo que afecta la seguridad del DBMS.

El manejador de la Base de Datos y el diccionario de datos usualmente proveen utilerías para revisar e imprimir las capacidades de acceso, información del usuario y bitácoras de auditorías.

***"Software"* del manejo de librerías.** Las funciones del *"software"* restringen el acceso a librerías críticas; los procedimientos que gobiernan el uso de esas funciones deberán ser revisados; evaluados y probados. El auditor deberá revisar, evaluar y probar lo siguiente:

- Documentación de librerías.
- Programas fuente(s) y ejecutables.
- *"Jobs"* en ejecución y lineamientos de control.
- Parámetros de corrida.
- Uso de *"software"* para restringir el acceso a librerías.
- Restricción del acceso a librerías de producción.
- Restricciones de funciones que pueden ser usadas para modificar el estado de un programa (pruebas a producción).
- Acceso a librerías en prueba.
- Convenciones para dar nombre a librerías que son usadas para facilitar la seguridad.
- Métodos para clasificar y restringir el acceso a librerías por tipo (fuentes, objeto, carga y control de *"job"*).

- Si el *"software"* ejecuta funciones de identificación de usuario y procedimientos de autentificación.
- Procedimientos inusuales de las librerías.
- Capacidades de la bitácora de auditoría.
- Los números de versión del *"software"*.

Los reportes escritos pueden ser usados para organizar las actividades de las librerías de *"logs"* de acceso al *"software"* manejador de librerías o bitácoras de auditoría.

***"Software"* de utilerías.** El auditor deberá evaluar, revisar y probar los siguientes procedimientos diseñados para limitar el acceso a comandos de utilerías o funciones:

- ✓ Funciones o comandos de utilerías.
- ✓ Los controles de acceso sobre comandos o funciones de utilerías.
- ✓ Seguridad de acceso a los programadores para la utilización de funciones o comandos de utilerías.
- ✓ Si el *"software"* ejecuta las funciones de identificación del usuario y procedimientos de autentificación.
- ✓ Capacidades de uso de utilería para cada grupo de usuarios.
- ✓ Bitácoras de auditorías.

El *"software"* de utilerías no provee bitácoras de auditoría, por ello debe usarse el reporte escrito del *"software"*, para lo cual puede utilizarse el *"software"* de control de acceso, si éste está integrado al *"software"*. Deberán usarse reportes para monitorear el control de acceso.

***"Software"* de telecomunicaciones.** El auditor deberá revisar, evaluar y probar si es posible usar las funciones del *"software"* que restringe el acceso en las redes de telecomunicaciones y los procedimientos que gobiernan su uso, especialmente los siguientes:

- Restricciones al acceso de la red basados en tiempo, día, usuario, lugar y terminal.
- Apagado automático de terminales inactivas en un tiempo específico (terminales que pueden ser usadas).
- Facilidad de acceso no autorizado basado en protocolos de transmisión y líneas para la conexión rápida.
- Números de seguridad de entrada (revisar la posibilidad de este número para acceso local o tableros de boletín nacional).
- "Autorrespuesta", facilidad de uso sobre módem.

- Horas durante las cuales la línea está disponible.
- Recursos y funciones posibles a través del acceso de entrada.
- Uso de identificación de la terminal físicamente.
- Controles de acceso sobre los recursos de la red.
- Controles de acceso sobre tablas de configuración de red.
- Controles de acceso a funciones de la red.
- Seguridad física sobre líneas telefónicas y telecomunicaciones.
- El uso de red de área local (LAN) y la conectividad para otras redes de área local (LAN), redes de área amplia (WAN) o redes en otro lugar.
- Si el *"software"* ejecuta las funciones de la identificación del usuario y procedimientos de autentificación.
- Procedimientos para la protección de comunicaciones (desde las conexiones hasta la recepción no autorizada).
- Posibilidad y uso de encriptación de datos o mensajes técnicos de identificación.

Los reportes escritos pueden ser usados para reportar las actividades de la red, de *"logs"* de acceso a *"software"* de telecomunicaciones o bitácoras de auditoría. Éstos pueden además hacerlo con el *"software"* de control de acceso. Los reportes especiales de auditoría deberán contener lo siguiente:

Personal registrado por el sistema en el que no corresponde la contraseña con su identificador, o el que ha intentado más de dos veces entrar al sistema sin una contraseña autorizada.

Identificaciones de usuarios no usados hace seis meses.

Identificaciones de usuarios con privilegios especiales.

Un reporte de referencias cruzadas que debe mostrar a los ID usuarios con cada acceso a las aplicaciones.

Listar todos los ID usuarios por grupos.

IV. 5.- Encriptamiento.

Encriptar es el arte de proteger la información transformándola con un determinado algoritmo dentro de un formato para queno pueda ser leída normalmente, (Derrien, 1994). Sólo aquellos usuarios que posean la clave de acceso podrán "desencriptar" un texto para que pueda ser leído. Las tecnologías modernas de encriptamiento hacen casi imposible que una persona no autorizada utilice la información.

Encriptar (Fisher, 2002), es la transformación de los datos a una forma en que no sea posible leerla por cualquier persona, a menos que cuente con la llave de descripción. Su propósito es asegurar la privacidad y mantener la información alejada de personal no autorizado, aun de aquellos que la puedan ver en forma encriptada.

Debido a que Internet y otras formas de comunicación electrónica se han convertido en algo normal y rutinario, la seguridad se ha convertido en un factor muy importante. El encriptamiento se usa para proteger mensajes de correo electrónico, firmas electrónicas, llaves de acceso, información de tipo financiero e información confidencial. Existen en el mercado diferentes paquetes y formas para encriptar la información.

Los sistemas de encriptamiento pueden ser clasificados en sistemas de llave simétrica, los cuales usan una llave común para el que envía información y para el que la recibe, y sistemas de llave pública, el cual utiliza dos llaves, una que es pública, conocida por todos, y otra que solamente conoce el receptor.

Para generar una firma digital, se usan algunos algoritmos públicos. La firma digital es un conjunto de datos que son creados usando una llave secreta, aunque existe una llave pública que es usada para verificar que la firma fue realmente generada usando la llave privada correspondiente. El algoritmo usado para generar la firma electrónica es de tal naturaleza, que si no se usa la llave secreta no es posible usar la firma electrónica.

La autenticación en sentido digital es el proceso por medio del cual el emisor y / o receptor de un mensaje digital confidencial tiene una identificación válida para enviar o recibir un mensaje. Los protocolos de autentificación pueden estar basados en sistemas convencionales de encriptamiento de llaves secretas, o en sistemas públicos de encriptamiento. En la autenticación de sistemas de llaves públicas se usan las firmas digitales.

La firma digital tiene la misma función que la firma escrita en cualquier documento. La firma digital es un fragmento de información confidencial y propia de cada usuario que asegura a la persona que envía o autoriza un documento. El receptor o terceras personas pueden verificar que el documento y la firma corresponden a la persona que lo firma, y que el documento no ha sido alterado.

La firma digital es usada para verificar que el mensaje realmente viene de la persona que se señala como la que lo envía. También puede ser usada para certificar que una persona envió un documento o una autorización en un tiempo determinado. Existe una serie de firmas digitales que identifican y certifican desde el usuario inicial hasta el último usuario. En el caso de envío de documentos pueden certificar la organización que envía el documento, su departamento y la persona que lo manda o autoriza.

Un sistema seguro de firmas digitales debe comprender dos partes: un método para firmar el documento que sea de tal manera confiable que no pueda ser usado por otras personas, y otro que verifique que la firma fue realmente generada por el que ella representa, de tal forma que posteriormente no pueda ser cuestionada.

El resultado de un conjunto de datos encriptados es la firma digital. Normalmente, junto con la información, la llave pública que es usada para firmar. Para verificar la información, el receptor primero determina si la llave pertenece a la persona a la cual debe pertenecer, y después de desencriptarla verifica si la información corresponde al mensaje, entonces la firma es aceptada como válida.

Criptoanálisis es el arte de desencriptar comunicaciones sin conocer las llaves apropiadas. Existen muchas técnicas para lograrlo, y entre las más comunes están:

- Ataque a textos encriptados. Ésta es una situación en la cual el atacante no conoce nada acerca del contenido del mensaje, y debe trabajar únicamente en el contenido del mensaje. En la práctica es muy posible adivinar el contenido de algún texto, ya que normalmente tienen encabezados fijos.
- Ataque conociendo el texto original. El atacante conoce o puede adivinar el contenido del texto debido a algunas partes del texto encriptado. El objetivo es desencriptar el resto deltexto usando esta información. Esto también puede ser hecho al determinar la llave usada para desencriptar
- Ataque hecho por medio de escoger un texto encriptado. El atacante tiene el objetivo de determinar la llave con la cual se encriptó el texto.
- Atacar en la parte central. Este tipo de ataque es relevante para la comunicación criptografiada y para los protocolos clave de intercambio. La idea es que cuando dos personas están intercambiando llaves de seguridad para lograr la comunicación, el atacante se pone en medio de la línea de comunicación. El atacante realiza un intercambio separado de laves. Posteriormente, el atacante, con las llaves de acceso, puede realizar cualquier función. Una forma de prever este tipo de ataques es encriptar la llave de acceso al momento de enviar, así, una vez enviada, el emisor y receptor verifican la firma digital para realizar las operaciones necesarias.
- Ataque en el tiempo. Éste es un nuevo tipo de ataque y está basado en la medición repetitiva de los tiempos exactos de ejecución.

Aunque existen diversas formas para atacar la información encriptada, es conveniente que el programador conozca las formas de encriptamiento, sus ventajas y desventajas , así como su costo, para determinar la mejor para cada uno de los sistemas, y que el auditor verifique la forma de encriptamiento y su seguridad de acuerdo con los requerimientos de seguridad de cada sistema.

Existen diferentes protocolos y estándares para la criptografía, entre los cuales están:

- DNSSEC (*Domain Name Server Security*). Éste es un Protocolo para servicio seguro de distribución de nombres.
- GSSAPI (*Generic Security Services, API*). Provee una autentificación genérica, llaves de intercambio e interfases de encriptamiento para diferentes temas y métodos de autentificación.
- SSL (*Secure Socket Layer*). Es uno de los dos protocolos para una conexión segura a la web.
- SHTTP (*Secure Hypertext Transfer Protocol*). Protocolo para dar más seguridad a las transacciones de web.
- E-Mail (*Security and Related Services*).
- MSP (*Message Security Protocol*).
- PKCS (*Public Key Encryption Standards*).
- SSH2 (*Protocol*).
- Algoritmos de Encriptamiento.
- DIFFIE HELLMAN.
- DSS (*Digital Signature Standard*).
- ELGAMAL.
- LUC.
- Symetricos.
- DES
- BLOWFISH.
- IDEA (*International Data Encryption Algorith*).
- RC4.

- Varios algoritmos de llave pública, algunos con promisorio futuro; sin embargo, el más popular es el RSA (*Rivest Shamir Adelman*). En algoritmos simétricos el más famoso es el denominado DES y su variante DES-CBC, pero el más reciente es RC4.

CAPÍTULO V.

INTERPRETACIÓN DE LA INFORMACIÓN.

V.1.- Técnicas para la Interpretación de la Información.

Para interpretar la información se puede utilizar desde técnicas muy sencillas hasta técnicas complejas de auditoría, (Coderre, 2000).

V.1.1.- Análisis Crítico de los Hechos.

Una de las primeras técnicas es el análisis crítico de los hechos. Esta técnica sirve para discriminar y evaluar la información; es una herramienta muy valiosa para la evaluación y se basa en la aplicación de las siguientes preguntas:

PREGUNTA.	FINALIDAD QUE DETERMINA.
Qué.	El propósito.
Dónde.	El lugar.
Cuándo.	El orden y el momento, sucesión.
Quién.	La persona.
Cómo.	Los medios.
Cuánto.	La cantidad.

La pregunta más importante es **qué**, pues la respuesta, permitirá saber si puede ser:

- ✓ Eliminada.
- ✓ Modificada o cambiada.
- ✓ Simplificada.

Las respuestas que se obtengan deben ser sometidas a una nueva pregunta: "¿Por qué?", la cual planteará un nuevo examen que habrá de justificar la información obtenida. Cada interrogante se debe descomponer de la siguiente manera:

1.- Propósito:

- Qué se hace.
- Por qué se hace.
- Qué otra cosa podría hacerse.
- Qué debería hacerse.

2.- Lugar:

- Dónde se hace.
- Por qué se hace allí.
- En qué otro lugar podría hacerse.
- Dónde debería hacerse.

3.- Sucesión:

- Cuándo se hace.
- Por qué se hace entonces.
- Cuándo podría hacerse.
- Cuándo deberá hacerse.

4.- Persona:

- Quién lo hace.
- Por qué lo hace esa persona.
- Qué otra persona podría hacerlo.
- Quién debería hacerlo.

5.- Medios:

- Cómo se hace.
- Por qué se hace de ese modo.
- De qué otro modo podría hacerse.
- Cómo debería hacerse.

6.- Cantidad:

- Cuánto se hace.
- Cuánto podría hacerse.
- Cuánto debería hacerse.

V.1.2.- Metodología para Obtener el Grado de Madurez del Sistema.

Para poder interpretar la información de los sistemas se debe evaluar el grado de madurez de los mismos, (Davies, 2001):

- ✓ Verificar si el sistema está definido.
- ✓ Verificar si el sistema está estructurado.
- ✓ Verificar si el sistema es relativamente estable.
- ✓ Verificar si los resultados son utilizados o no.

CARACTERÍSTICAS.	MADURO	INMADURO.
Definido.	Completamente.	Incompleto.
Estructurado.	Alta.	Baja.
Estable.	No cambia.	Muchos cambios.
Resultados.	Utilizados.	No utilizado.

Dependiendo del grado de madurez y de su grado de estructuración, se determina si debe estar automatizado y la posible madurez que repercutirá en una mejor utilización y en disminución de cambios. Si el sistema está estructurado y maduro se debió seguir haciendo manualmente; si está semiestructurado y maduro se podrá usar la técnica de soporte en la toma de las decisiones (DSS, *Decision System Support*).

Si el sistema está semiestructurado pero no está maduro debió seguirse haciendo en forma manual; si no está estructurado y maduro, es un sistema guiado por la intuición y deberá seguirse haciendo en forma manual. Si no está estructurado ni maduro, el sistema no tiene razón de existir.

Nivel de Madurez.	Maduro.	Inmaduro.
Nivel de Estructura.	Estructurado.	Sistema de Información General.
Semiestructurado.	Sistema de Soporte.	Manual de Decisiones.
No Estructurado.	Intuitivo.	Sin Razón.

V.1.2.1.- Uso de Diagramas.

Otra forma de analizar los hechos es seguir la ruta de la información desde su origen hasta su destino, y disponer de este camino en una secuencia cronológica, con el fin de clarificar dónde aparece, cómo avanza a lo largo del sistema y cómo llega a su destino. Esta técnica ayuda a hacer un estudio objetivo de todos los pasos por los cuales deberá pasar la información. Se considera necesario agregar algunas características que definan aún más este estudio como: frecuencia, tiempo, costo y distancia física de cada paso coadyuvando a una evaluación más objetiva del sistema, según Graham (1993).

V.2 .- Evaluación de los Sistemas.

Se debe evaluar el desarrollo que ha tenido el sistema mediante el análisis de los pasos que comprendió el desarrollo del sistema, y comparar lo que se planeó contra lo que realmente se está obteniendo, (Henry, 1995).

V.2.1.- Análisis.

Se debe evaluar la información obtenida en los sistemas para poder.

- Determinar el objeto y compararlo con lo obtenido.
- Buscar la interrelación con otros sistemas.
- Evaluar la secuencia y flujo de las interacciones.
- Evaluar la satisfacción del usuario.

Entre las etapas del análisis están:

1.- Análisis conceptual:

- Evaluar el sistema funcional.
- Evaluar la modularidad del sistema.
- Evaluar la segmentación del sistema.
- Evaluar la fragmentación del sistema.
- Evaluar la madurez del sistema.
- Evaluar los objetivos particulares del sistema.
- Evaluar el flujo actual de información.
- Definir el contenido de los reportes y compararlo con el objetivo.

2.- Evaluar los modelos de reportes:

- Evaluar los controles de operación.
- Cuantificar el volumen de información.
- Evaluar la presentación y ajustes.

Se debe conocer en términos generales el nivel del sistema funcional para obtener los elementos suficientes que permitan evaluar el nivel de interacción, su grado de estructuración y la madurez del sistema con el fin de determinar si se justifica su automatización.

Entre las evaluaciones que deben hacerse están:

Evaluar el objetivo. Evaluar que el objetivo general y el alcance del sistema funcional estén definidos en forma clara y precisa. Esta actividad se encarga de delimitar el sistema obteniendo todo lo relacionado con él, mediante las entrevistas a los usuarios involucrados con el fin de evaluar si se cumplió con el objetivo. Las versiones que ofrezcan los usuarios deberán ser confrontadas para verificar su compatibilidad.

Evaluar la interacción con otros sistemas. Se debió analizar la información del sistema con el propósito de localizar sus interacciones y sus contactos con otros sistemas, a fin de determinar si existe un sistema integral de información, sistemas aislados o simplemente programas, o si existe redundancia y ruido, así como cuáles son los controles con que cuenta el sistema. Para evaluar todas las entradas y salidas que tienen lugar en el sistema, esta parte de la auditoría determina el flujo de operación y también todas las entradas y salidas que ocurren internamente. La manera de desarrollar esta actividad es usar aquellos documentos de información que maneja el sistema, rastreando las fuentes y destinos, elaborando o reservando la matriz de recepción / distribución de los documentos y la matriz de entradas / salidas.

Evaluar si se obtiene la secuencia y flujo de las interacciones. Para llevar a cabo esta actividad es necesario establecer el flujo de información a través del sistema, tomas de la matriz de entradas / salidas y agregar el orden de ocurrencia, así como la periodicidad. Graficándola en un plano horizontal para tratar de encontrar duplicidad de información. Este plano debe hacerse de tal manera que refleje un período, así como el orden de ocurrencia.

Evaluar el sistema funcional. Dado que ya se evaluó el objetivo, las interacciones y su flujo, lo que sigue es analizarlo para tener una idea más clara de su función. Tomando como base los elementos de los primeros tres pasos, se debe verificar si es congruente con su objetivo; es decir, si la descripción define sus propósitos. En esta etapa se evalúa "qué hace" el sistema.

Evaluar la modularidad del sistema. Esta actividad subdivide el sistema en partes que pueden ser procesadas en forma independiente, pero cuyo objetivo particular es buscar el objetivo general del sistema funcional, correspondiendo a cada módulo una función general del sistema. Así mismo, una función general del sistema consiste en identificar aquellas partes de éste donde ocurre una entrada, un proceso, y se obtiene un resultado parcial.

Evaluar la segmentación del sistema. Este paso tiene por objetivo subdividir los módulos en funciones particulares, de tal manera que el conjunto de funciones defina al módulo en cuestión. En esta parte deben evaluarse aquellas funciones que son realizadas para distintos módulos (interconexión modular), cada función extraída del módulo debió ser consistente y validada por con el usuario.

Evaluar la fragmentación del sistema. Se subdivide el segmento en funciones específicas o procedimientos, pues cada función particular o segmento puede contener uno o más procedimientos. A su vez, cada procedimiento puede estar formado por distintos niveles(jerarquía de procedimientos); dependiendo de su complejidad en esta parte se debe evaluar haciendo énfasis en "qué se hace" y no en el "cómo se hace", ya que esto se evalúa en el análisis detallado.

Evaluar el flujo de información del sistema funcional. Identificar en cada documento su origen y su seguimiento a través de las diferentes entidades o departamentos por donde transita; a la vez vaya identificándose las adiciones y supresiones de información. Por último, se identifica como y dónde llega a su destino. Se recomienda el uso del diagrama de flujo de información.

Una forma de analizar los hechos es seguir la ruta de la información desde su origen hasta su destino y disponer de este camino en una secuencia cronológica con el fin de clasificar dónde aparece, como avanza a lo largo del sistema y cómo llega a su destino. Esta técnica ayuda a hacer un estudio objetivo de todos los pasos por los cuales deberá pasar la información. Se considera necesario agregar algunas características que definan aún más este estudio, como frecuencia, volumen, tiempo, costo y distancia física de cada paso, lo cual ayudara a un mejor análisis y a una evaluación más objetiva del sistema.

Evaluar los documentos de entrada y el contenido de los reportes. Se deben evaluar las formas de entrada, su contenido, claridad, controles, copias solicitadas y autorizaciones, verificar que los reportes o pantallas de salida contengan todos los datos necesarios sin importar de dónde provienen. El uso que se le da, quien los prepara y a quien va dirigidos.

Evaluar los controles de operación del sistema. Se debe evaluar claramente en qué parte del proceso operacional se llevan a cabo los controles, analizando sobre que variables se ejerce y cómo se ejerce (procedimientos), así como las acciones a tomar en cada situación dada, es decir, se evalúa su razón de ser, su método y su grado de sensibilidad.

Cuantificar el volumen de información que se manejará. La importancia este paso es tener una idea aproximada de los recursos que se necesitan, si están siendo usados correctamente, la situación del equipo y la posibilidad de incremento de equipo. Esto de obtiene sumando los caracteres involucrados en los reportes y documentos utilizados, especificando el número de veces que ocurre cada rubro y la longitud de ellos.

El sistema deberá tener las siguientes características:

- Generalidad. Que busca objetivos amplios pensando en que las mejoras pueden ser hechas en cualquier momento.
- Flexible. Que pueda ser adaptable a las circunstancias cambiantes.
- Portabilidad. Que pueda ser susceptible de ser implantado en diferentes ambientes y equipos.
- Confiabilidad. Esto es, que sea capaz de detectar posibles errores para que éstos no se procesen.
- Seguridad. Que el sistema cuente con dispositivos para que sólo la gente autorizada pueda tener acceso a la información.
- Fácil de usarse y operable. Que tenga capacidad para recuperarse de una falla del equipo.
- Confidencialidad. Accesible solo para aquellas personas autorizadas para su manejo, consulta y exploración.
- Modificable. Que se traducen en la capacidad del sistema para adiciones, sustituciones o eliminaciones de elementos con el fin de efectuar nuevas funciones o dejar de efectuar otras, sin alterarse las que no se deseen.

Evaluar los archivos. Analizar a detalle los archivos de información involucrados en el sistema, y señale sus atributos y propiedades, su estructura, clasificación , organización, frecuencia de uso, campos, códigos, tamaño. Se recomienda hacer referencia a los programas que lo usan.

Evaluar los reportes. Se evaluarán las formas de salida de los reportes, o sea la infraestructura, mediante el diseño de la forma y la distribución de su contenido validándola con el usuario:

Programa que lo genera.
Archivos usados.
Frecuencia.
Usuario.
Contenido.

Pruebas y revisiones. El objetivo es asegurarse que el sistema funciones de acuerdo con las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación (utilizar la información obtenida en las opiniones de los usuarios). Esta actividad es muy importante ya que el costo de corregir errores es directamente proporcional al momento que se detecta. Las pruebas del sistema buscan asegurar que se cumplan los requisitos de las especificaciones funcionales, verificando datos estadísticos, transacciones, reportes, archivos, anotando las fallas que pudieran ocurrir, y realizando los ajustes necesarios. Los niveles de prueba pueden ser agrupados en módulos, programas y en el sistema total.

V.3 .- Evaluación de los Sistemas de Información.

Esta función tiene una gran importancia en el ciclo de evaluación de las aplicaciones del sistema de información por computadora. Busca comprobar que la aplicación cumpla con las especificaciones requeridas por el usuario, que se haya desarrollado dentro de lo presupuestado y que efectivamente cumpla con los objetivos y beneficios esperados, (Hernando, 1997).

Un cambio a un sistema existente, como la creación de uno nuevo, introduce necesariamente cambios en la forma de obtener la información y un costo adicional. Ambos deberán ser evaluados antes y después del desarrollo.

Se debe evaluar el cambio (si lo hay) de la forma en que las operaciones son ejecutadas, comprobar si mejora la exactitud de la información generada, si la obtención de los reportes efectivamente reduce en tiempo de entrega, si es más completa, en que tanto afecta las actividades del personal usuario, si aumenta o disminuye el personal de la organización, y los cambios de las interacciones entre los miembros de la organización. De ese modo se sabrá si aumenta o disminuye el esfuerzo por generar la información para la toma de decisiones, con el objeto de estar en condiciones de determinar la productividad y calidad del sistema.

El análisis deberá proporcionar: la descripción del funcionamiento del sistema desde el punto de vista del usuario, indicando todas las interacciones del sistema, la descripción lógica de cada dato, las estructuras que forman estos y el flujo de información que tiene lugar en el sistema; lo que el sistema tomará como entradas, los procesos que serán realizados, así como las salidas que deberán proporcionar, los controles que se efectuarán para cada variable y los procedimientos.

De este modo se agruparan en cuatro grandes temas:

- Evaluación en la ejecución.
- Evaluación en el impacto.
- Evaluación económica.
- Evaluación subjetiva.

V.3.1 .- Evaluación en la Ejecución.

Se refiere al uso de cuestionarios para recabar datos acerca de la actuación de la aplicación en la computadora, con objeto de conocer qué tan bien o qué tan mal está siendo usada y se opera eficientemente.

Los cuestionarios son medios para recopilar datos acerca del uso de los recursos de la computadora y pueden ser cuestionarios, manuales, encuestas de opiniones, evaluación de documentación, obtención de información, electrónica integrada al equipo (*"hardware"*) y de programas ejecutándose (*"software"*), obteniéndose en ambas las estadísticas acerca de su uso, (Hevia, 1990).

Los dispositivos de *"hardware"* son dispositivos electrónicos que pueden ser conectados a varios puntos del equipo, como lo son en la unidad de control, los canales de comunicación, etcétera, que durante la ejecución de una aplicación registran cantidad, frecuencia y dirección de los componentes del equipo. Los datos son almacenados normalmente sobre cinta magnética o disco, para que puedan ser analizados después; por ejemplo, algunos de esto contabilizan la frecuencia de uso de la unidad central de proceso en relación con la espera para operaciones de entrada-salida. Analizando estos datos quizá se detecte la necesidad de agregar procesadores de entrada-salida con objeto de acortar la espera de procesador central, eliminando los cuellos de botella que por esta causa se generan.

Las estadísticas de *"software"* son juegos de instrucciones ejecutables conectadas al sistema operativo con el fin de colectar datos acerca de la operación del sistema y acerca de los programas de aplicación. Este tipo de monitor requiere memoria y proceso adicional, lo que disminuye la rapidez del procesador. Los datos también son almacenados en cinta magnética o cualquier otro dispositivo de almacenamiento secundario con el fin de analizarlos después. Este monitoreo ayuda a detectar que recursos adicionales se necesitan o que recursos existentes deben ser ejecutados para lograr mas eficiencia.

Una estadística de *"hardware"* puede ser utilizada para medir la cantidad de tiempo de la unidad de procesamiento central, pero también podrá ser concentrada en los canales de comunicación y dispositivos de almacenamiento secundario para determinar la frecuencia y cantidad utilizada. Su importancia se puede evaluar con el siguiente ejemplo:

Si se está considerando agregar una nueva aplicación al sistema, el análisis del monitoreo ayuda a determinar si la computadora podrá soportarla, si puede ayudar al administrador a decidir si se agregan nuevas unidades de almacenamiento, líneas de comunicación, terminales, etcétera. Así mismo, puede usarse para determinar si todo el equipo es necesario, si se deben rediseñar los archivos, etcétera.

Las estadísticas del *"software"* ayudan a identificar cuales son los lenguajes más usados, que tipo de proceso es más común (alto volumen de actualizaciones contra secuencia de cálculos, complejos procesos en lotes contra procesos en línea, frecuencia de corridas, de pruebas, programas terminados anormalmente, etcétera).

Estas evaluaciones son generadas automáticamente mostrando a que horas del día los trabajos son corridos y también que recursos del sistema fueron utilizados y que tan grandes son las aplicaciones en relación con el equipo.

Basándose en estos datos, el auditor contará con la información necesaria para hacer las evaluaciones tendientes a mejorar el servicio o incrementar la eficiencia.

Estos dos tipos de monitores normalmente son proporcionados por el fabricante de ordenadores, pero algunos monitores de *"software"* pueden ser desarrollados por la propia organización.

V.3.2 .- Evaluación en el Impacto.

Es la evaluación que se hace sobre la manera en que afecta a la gente que interviene en la aplicación (usuarios) con el objeto de determinar cómo la implantación y el uso del sistema de información afecta a la organización distinguiendo que factores son directamente atribuibles al sistema. Las principales áreas que deben interesar son las que intervienen en la toma de decisiones y en las actividades de operación, (Martin, 2000).

Esta evaluación se hace con el fin de detectar a la gente involucrada; las actividades que son necesarias realizar, la calidad de la información, y el costo de operación resultante.

Alguna expectativas deben ser elaboradas y jerarquizadas antes de empezar a diseñar el sistema con el fin de que, cuando se instale, se compruebe si los resultados satisfacen plenamente lo planeado. Estos datos también son importantes para guiar futuros proyectos.

Así mismo se debe evaluar el efecto que tiene sobre el ambiente del sistema (personas, leyes, etcétera). Para ello se cuenta con varias técnicas que ayudan para este propósito, las cuales son: bitácora de eventos, registro de actitudes, contribución, peso y análisis de sistemas.

Bitácora de eventos.

Esta información se obtuvo en la sección de la opinión del usuario donde se registraron los eventos relacionados con la introducción de una aplicación. Cualquier evento que influya en el sistema y cualquier nuevo evento introducido por él, es registrado en forma de notas, y al final se agrupan. Para un estudio sistemático no se requiere equipo adicional, y debe usarse cuando la medición tiene lugar en periodos largos o cuando se desean medir varios tipos de impactos. Va enfocado a usuarios y a gente de sistemas antes y después de implantar la aplicación.

Registro de actitudes.

Éste se concentra a obtener datos acerca de opiniones e ideas individuales de los usuarios de los sistemas de información a través de cuestionarios, con el objeto de poder mejorarlos o detectar deficiencias. Ésta técnica es usada cuando existen algunas medidas cuantificables, observaciones concretas o ambas cosas.

Contribución y peso.

Esta técnica requiere que se desarrolle previamente un juego de parámetros o factores relacionados con el impacto del sistema de información, como facilidad de uso, rapidez de recuperación de datos, claridad, exactitud, etcétera. Una vez que éstos son identificados, se ordenan por importancia en forma de cuestionarios, para definir términos de escala de valores, que pueden ser muy buenos o muy malos.

Esta técnica proporciona una completa valoración de lo que el usuario siente de cada factor, con lo que se puede comparar entre varios usuarios y también entre usuario-gente de sistemas. Ayuda a rediseñar nuevas características del sistema que se hubiera pasado por alto, así mismo contribuye a retroalimentar el funcionamiento de la aplicación.

Análisis de sistemas.

Cuando se utiliza para evaluar el impacto, el análisis se enfoca al uso del sistema una vez instalado. Este enfoque ayuda a estudiar como el sistema afecta la estructura de la organización, los procedimientos y, en general, las políticas de la organización. Se analizan los mismos factores del sistema que se analizaron antes del diseño. Esta técnica se usa para evaluar el impacto para la preparación, uso de reportes y el resultado de las decisiones.

V.3.3 .- Evaluación Económica.

La evaluación económica es la actividad que se encarga de obtener el costo de una aplicación y cuantificar los beneficios esperados con el objeto de justificar o no su desarrollo, o comprobar que la aplicación se desarrolló según lo presupuestado. Ello a de ser considerado para el auditor para evaluar el impacto económico del sistema dentro de la organización en elación con los beneficios obtenidos por éste.

En el impacto se mide cómo una aplicación del sistema de información a contribuido a mejorar la eficiencia en el área donde se usa. Así mismo la evaluación después de su implementación es crítica para conocer cómo el sistema opera y dónde pueden necesitarse cambios, (Meyer, 2002).

La evaluación económica es importante puesto que el capital y la organización no son gratuitos, debiéndose cuantificar los beneficios y los costos del sistema en términos monetarios para estar en condiciones de justificar o no su desarrollo e implantación.

Cuando la aplicación a sido realizada, se busca obtener el costo real contra el beneficio real para comprobar o determinar el por qué de la diferencia con lo presupuestado y / o la calidad de la aplicación.

Estas técnicas ayudan a obtener los elementos necesarios para evaluar por medio de un análisis de costo / beneficio de la aplicación. Permite además evaluar si fue desarrollado en las condiciones económicas esperadas, por lo que este análisis deberá efectuarse antes y después del desarrollo de la aplicación. La justificación se encuentra en el hecho de que cualquier tipo de organización busca alcanzar sus objetivos con recursos económicos limitados.

El administrador del sistema de información deberá verificar y cuidar que estas actividades se realicen en forma sistemática y completa para evitar crear sistemas que perjudiquen a la organización y minen su economía.

Este punto es de suma importancia dado el momento actual en donde los recursos computacionales se ven afectados constantemente por la devaluaciones y el costo del capital. Hay que tratar de obtener el mayor beneficio con el equipo disponible e invertir en equipos adicionales sólo cuando esté plenamente justificada la inversión por los beneficios que se obtendrán.

V.3.4 .- Evaluación Subjetiva.

Partiendo de la premisa de que los usuarios son los principales afectados directamente por el sistema, sus puntos de vista y necesidades deberán ser considerados para la evaluación.

Los que procesan los datos, el personal de sistemas y el personal de alta dirección deberá también participar en la determinación de los beneficios económicos de la actividad particular a ser desarrollada.

Un enfoque experimental propone un mecanismo para obtener los factores. Además de ahorro de costos, que habrán de ser considerados e la evaluación del sistema de información.

Se necesita incorporar puntos de vista y opiniones de la gente que usará o será afectada por la aplicación del sistema de información.

La justificación de evaluación subjetiva se centra en que la opinión del grupo usuario proporciona un punto de vista más completo de la aplicación, ayudando a obtener aquellos factores que se hubiere pasado por alto.

Un procedimiento de la evaluación subjetiva es el uso de cuestionarios que se aplicarán a un grupo de administradores, usuarios y personal de sistemas para contestar una secuencia de preguntas que a la larga dejan una contribución en pesos. Incluyen especificaciones detalladas de la intención del proyecto y simples respuestas; no hay referencia en costos, solo se estiman los beneficios.

Estas preguntas serán proporcionadas a los miembros del grupo, en varios tiempos o etapas, y todos reciben retroalimentación de las respuestas de otros miembros, entre cada ronda de preguntas. La gente entonces puede cambiar sus evaluaciones y aclarara su retroalimentación; se puede saber quién formuló las evaluaciones y su nivel. El proyecto es evaluado en términos de cuanto pagaría por la información sin hacer referencia a términos vagos para su valoración.

Otro método es por medio del desarrollo de una metodología que mida el valor de la información generada por la aplicación y la ganancia de su uso, esto implicaría un valor estimado por el usuario de los posibles beneficios.

Usando la estimación subjetiva es posible obtener diversas opiniones dentro del informe mientras se obliga a los miembros del grupo a examinar sus propios razonamientos acerca de la aplicación a través de la retroalimentación de otras opiniones. Este método se centra en la pregunta: "¿Cuánto pagaría por esta información?" y no en "¿Cuál es el valor de la información?", la cual descansa sobre la mala definición y dificultad para comprender el concepto del valor de la información.

Para poder contestar estas preguntas el auditor deberá acatar la tarea de determinar cuanto dinero le cuesta a la organización asignar el proyecto especifico y poder compararlo con otros proyectos (costo de oportunidad).

V.3.5 .- Controles.

Un punto muy importante a considerar dentro de la auditoria son los controles, los cuales se dividen en generales, operativos (dependiendo del sistema) y técnicos (equipos y sistemas).

Los controles generales normalmente se aplican a todo el procedimiento de la información y son independientes de las aplicaciones, estos controles incluyen:

- Planeación.
- Organización.
- Política y procedimientos.
- Estándares.
- Administración de Recursos.
- Seguridad.
- Confiabilidad.

Los controles operativos comprenden cada uno de los sistemas en forma individual y constan de:

- Control de flujo de la información.
- Control de proyectos.
- Organización del proyecto.
- Reportes de avance.
- Revisiones del diseño del sistema.
- Técnicas:
    - De usuario.
    - De control.

- Control de cambios a programas:
    - Requisición de cambio.
    - Razón de cambio.
    - Naturaleza del cambio.
    - Persona que lo solicita.
    - Persona que revisa y autoriza.
    - Frecuencia de cambios.
    - Persona asignada al mantenimiento.
    - Bitácora de cambios.

- Mantenimiento y documentación.
- Producción.
- Controles de documentación.
- Documentación.
    - Del sistema.
    - Del programa.

- Mantenimiento y acceso a la documentación.
- Control de sistemas y programas.
- Sistemas de lote.
    - De entrada.
    - Autorización de entrada.
    - Armado de lotes.
    - Verificación de lotes.

- Control de programas.
- Reporte de control:
    - Balanceo de lotes.
    - Reporte de errores.
    - Reporte de excepción.
    - Reporte de transacciones.
    - Reporte de cambios de archivo maestro.
- Validación de entradas:
    - Verificación de secuencia.
    - Campos omitidos.
    - Totales de control.
    - Transacciones válidas.
    - Caracteres válidos.
    - Códigos válidos.
    - Pruebas de razonabilidad.
    - Dígito verificados.
    - Etiquetado de archivos.

- Controles de programas misceláneos:
    - Control de programa a programa.
    - Verificación de etiquetas.
    - Intervención del operador.
    - Punto de verificación y reinicio.
    - Control de salida.
    - Formato de salida.
    - Control de formas de salidas.
    - Corrección de errores.
    - Controles corrida a corrida.
    - Sistemas de línea.
- Controles de entrada:
    - Acceso a terminales.
    - Acceso a programas, archivos, datos y al Ordenador.
    - Comunicaciones.
    - Información confidencial.
- Control de programas:
    - Reportes de control.
    - Validación de entrada.
- Corrección de errores.
- Puntos de verificación y reinicio.
- Controles de salida:
    - Formatos de reporte.
    - Formas de control de salida.
    - Información confidencial.

Los controles técnicos que se deben evaluar son:

- Controles de operación.
- Supervisor.
- Capturista.
- Bibliotecario.
- Operadores.
- Controles d entrada y salida.
- Recepción de información.
- Detección y corrección de errores.
- Distribución de la información.
- Calendarización.

- Reporte de fallas y mantenimiento preventivo.
- Controles sobre archivos.
- Recuperación de desastres.
- Controles de usuarios.
- De origen de datos.
- Origen de documentación fuente.
- Automatización de documentación fuente.
- Recolección y preparación de entrada y documentación fuente.
- Manejo de errores de documentación fuente:

    - Tipos de errores que pueden aparecer.
    - Pasos a seguir para su corrección.

Los métodos a utilizar para recuperara documentos fuente corregidos son:

- Retención de documentos fuente.
- Controles de entrada de datos.
- Conversión de datos y captura.
- Validación de datos.
- Manejo de errores en datos y captura.
- Controles de salida de datos.
- Balanceo y conciliación de salidas.
- Distribución de salidas.
- Procedimientos documentados que describen los métodos de distribución.
- Calendarización, revisión y distribución de salida por parte de los usuarios.
- Bitácoras de reportes.
- Manejo de retención de registros de salida y documentos contables.
- Formatos de salida:

    - Frecuencia.
    - Número de copias.

Controles técnicos:

- Programática.
- Aplicaciones.
- Sistemas.

Recursos de los programas por aplicación:

- Calendario de programas.
- Errores y recuperación.

Registro contables:

- Equipos.
- Unidad de control de procesos.
- Memoria secundaria.
- Dispositivos periféricos.

Controles lógicos del sistema.

- Sistemas operativos.
- Sistemas de utilerías.
- Sistemas de biblioteca.
- Sistemas de mantenimiento de archivo.
- Sistemas de seguridad.

Control de acceso al sistema.

Control de cambios al sistema:

- Redundancia en la información.
- Inconsistencia de datos.
- Seguridad.

Controles de seguridad, respaldo y confidencialidad.

Sobre las bases de los objetivos de la auditoria en informática se deben presentar, de acuerdo con la información obtenida, los controles existentes, las conclusiones, opiniones y alternativas de solución debidamente fundamentadas en cuanto a:

- Evaluación de los sistemas.
- Evaluación de los equipos.

V.3.6 .- Presentación.

La presentación de las conclusiones de la auditoría podrá hacerse en la siguiente forma:

1.- Una breve descripción de la situación actual en la cual se reflejen los puntos más importantes. (Esta presentación es para el nivel más alto de la organización).

2.- Una descripción detallada que comprende:

- Los problemas detectados.
- Posibles causas, problemas y fallas que originaron la situación presentada.
- Repercusiones que pueden tener los problemas detectados.
- Alternativas de solución.
- Comentarios y observaciones de la dirección de informática y de los usuarios sobre las soluciones propuestas.

Si se opta por alguna alternativa de solución, cuáles son sus repercusiones, ventajas y desventajas, y tiempo estimado para efectuar el cambio.

1.- Se debe hacer hincapié en cómo se corregirá el problema o se mejorará una determinada situación, se obtendrán los beneficios, en cuánto tiempo y cuáles son los puntos débiles.

2.- Se debe romper la resistencia a la lectura que tienen algunos ejecutivos por medio de conclusiones concretas que sean sencillas (se procurará que se entiendan los términos técnicos y, si es posible, usar técnicas audiovisuales).

Cómo ejemplo de formato de presentación de las conclusiones de la Auditoría en Informática, véase la Figura V.1, y como ejemplo del seguimiento de la Auditoría en Informática, véase la Figura V.2.

Conclusiones de la auditoría en informática

DIRECCION _____ HOJA NUM _____ DE _____

AUDITORIA A _____ FECHA DE TERMINO DE LA AUDITORIA _____

NUM	PROBLEMATICA	CAUSAS	REPERCUSIONES	ALTERNATIVAS DE SOLUCION	OBSERVACIONES	FECHA PROBAS IMPLAN	RESPONS DE LA RECOMEN

Figura V.1.- Conclusiones de la Auditoría Informática.

Seguimiento de las recomendaciones de la auditoria en informatica

PERIODO QUE SE REPORTA _____

DIRECCIÓN _____ HOJA NUM _____ DE _____

AUDITORIA A _____ FECHA DE TERMINO DE LA AUDITORIA _____

NUM OBS	RECOMENDACIÓN	FECHA ESTIMADA DE RESOL	FECHA REAL DE RESOL	MOTIVO POR EL CUAL NO HA SIDO RESUELTA	REPLANTEAMIENTO DE LA SOLUCIÓN	OBSERVACIÓN	FECHA APROBADA IMPLAN	RESPONS DE LA RECOMEN

Figura V.2.- Seguimiento de las Recomendaciones de la Auditoria en Informática.

CONCLUSIONES.

El avance tecnológico que se ha logrado en los últimos años ha sido impresionante. El avance se ha reflejado más posiblemente en el Área de Informática, lo cual ha provocado que se tenga microordenadores con un bajo costo y con gran capacidad de procesamiento y que se cuente con ordenadores que permitan desde el control del proceso de ensamble de automóviles en forma completamente automática, hasta que en la década de los sesenta se haya podido llegar a la Luna. En el área educativa este avance ha influido en todas las carreras, desde las subtécnicas y subprofesionales hasta las técnicas y profesionales. Nos encontramos así con que los niños de primaria ya están usando los ordenadores y no hay profesión que no necesite en forma directa o indirecta su utilización.

Si analizamos que aproximadamente ochenta por ciento de los ordenadores digitales son utilizadas en las organizaciones con fines de información, de toma de decisiones, contables y administrativos, y si evaluamos el costo que representa la utilización de estos ordenadores, podremos ver la importancia que tiene para la alta dirección poder evaluar la adecuada utilización de esta herramienta.

Esto trae como consecuencia que el profesional deba actualizarse en el uso adecuado de la nueva tecnología, así como en la evaluación que se haga de este recurso tan costoso. También deben adecuarse las Normas de auditoría y del control interno para que sean congruentes con el desarrollo tecnológico. La Auditoría en Informática es una nueva materia que es consecuencia directa del desarrollo en el área y de la necesidad de evaluar la adecuada utilización, respaldo y confidencial de la información de la organización.

Esta nueva área evalúa la información desde su generación (dato) hasta su utilización (información), y debe considerar la herramienta que se utiliza, su optimización, el respaldo de la información, la seguridad y confidencialidad de la misma y conseguir el mejor uso de la información al menor costo, evitando duplicidad.

Para lograr esta evaluación se requiere que el auditor conozca no sólo sobre las materias que le son propias, sino que tenga una capacidad técnica en el área de sistemas computacionales e informática.

La auditoría no debe terminar con la presentación, sino ser el inicio de una serie de auditorías y revisiones periódicas, con un adecuado seguimiento de las observaciones, para lograr las correcciones a los problemas y las mejoras a los sistemas que lo ameriten.

BIBLIOGRAFÍA.

Abrams, M. y Jajodia, S. (1995). **Information Security.** USA: IEEE Computer Security Press.

Acha Iturmendi, J. (1994). **Auditoría Informática en la Empresa.** Madrid: Paraninfo.

Almela Díez y Castaño Viedma. (2002). **El Riesgo de la Auditoría y la Materialidad.** Valencia: Institut de Cultura Juan Gil-Albert. Generalitat Valenciana.

Alonso Rivas, Gonzalo. (1989). **Auditoría Informática.** Madrid: Díaz de Santos Editores.

Álvarez Anguiano, Jorge. (1998). **Apuntes de Auditoría Administrativa.** México: Facultad de Contaduría y Administración. UNAM.

Arkin, H. (2000). **Handbook of Sampling for Auditing and Accounting.** New York: Mc Graw-Hill.

Bacard, André. (2002). **The Computer Privacy Handbook.** New York: Peachpit Press.

Baker, R. (2000). **The Computer Security Handbook.** New York: TAB Professional and Reference Books.

Barriusco Ruíz, Carlos. (1996). **Interacción del Derecho y de la Informática.** Madrid: Dykinson.

Bernal Montañés, Rafael y Coltell Simón, Óscar. (1997). **Auditoría de los Sistemas de Información.** España: Universidad Politécnica de Valencia.

Brandon, Dick. (2002). **Management Standards for Data Processing.** New York: Van Nostrand Reinhoold Company.

Caballero, P. (1996). **Introducción a la Criptografía.** Madrid: Textos Universitarios Ra-ma.

Calle Guglieri, J. A. (1997). **Reingeniería y Seguridad en el Ciberespacio.** Madrid: Díaz Santos Editores.

Centro de Informática de la Facultad de Contaduría y Administración. (1983). **Boletín del Centro de Informática de la FCA de la Universidad Nacional Autónoma de México.** México: UNAM.

Coderre, David. (2000). **Coats and others Beasts for Auditors.** Vancouver: Global Audit Publications.

Coelli, William. (2002). **Information Security Handbook.** New Jersey: Macmillan Publishers, Ltd.

Davies, D. (2001). **Security for Computer Networks.** New York: John Wiley & Sons.

Derrien, Y. (1994). **Técnicas de Auditoria Informática.** Barcelona: Marcombó.

Derrien, Yan. (2000). **Técnicas de la Auditoria en Informática.** México: Alfaomega Marcombó.

Dorf, R. y Bishop, H. (1995). **Modern Control Systems.** New York: Addisson Wesley.

Echenique García, José. (2001). **Auditoria en Informática.** México: Mc Graw-Hill, 2° Edición.

Fantinatti, J. (2000). **Seguridad en Informática.** México: Mc Graw-Hill.

Fernández Arenas, José. (2001). **La Auditoria Administrativa e Informática.** México: Diana.

Fine, H. (1998). **Seguridad en Centros de Cómputo.** México: Trillas.

Fisher, R. P. (2002). **Seguridad en los Sistemas Informáticos.** Madrid: Díaz de Santos Editores.

Fundación Arturo Rosemblueth. (2000). **La Computación en México: Diagnóstico, Perspectiva y Estrategia de Desarrollo.** México: Editorial de la Fundación Arturo Rosemblueth.

Graham Dougalll, E. (1993). **Computer Security.** Amsterdam: IFIP.

Gratton, Pierre. (1998). **Protección Informática.** México: Trillas.

Haag, Steven. (2000). **Management Information Systems.** New York: Mc Graw-Hill.

Henry, M. (1995). **Practical Computer Network Security.** New Jersey: Artech House.

Hernández Hernández, Enrique. (1996). **Auditoría en Informática, un Enfoque Metodológico y Práctico.** México: Continental.

Hernando Collazos, Isabel. (1997). **Productos Multimedia y Derechos de Autor.** San Sebastián: Editorial L. C.

Hevia, Eduardo. (1990). **Manual de Auditoría Interna: Enfoque Operativo y de Gestión.** España: Biblioteca Master Centrum.

I.F.I.P. (1990). **Procedings of the Sixth IFIP. International Conference on Computer Security and Information Integrity.** Helsinki: IFIP.

Instituto Mexicano de Contadores Públicos. (2000). **Control y Auditoría del Computador.** México: Instituto Mexicano de Contadores Públicos A. C.

Instituto Mexicano de Contadores. (2001). **El Boletín C de Normas de Auditoría.** México: IMC.

Instituto Mexicano de Contadores. (2002). **El Boletín E-02.** México: IMC.

Jalife Daher, Mauricio. (2002). Secretos Industriales: **Comentarios sobre Aspectos Relevantes de su Reglamentación en México.** México: Trillas.

Knudson, H. y Woodworth, R. (2002). **Management An Experimental Approach.** New York: Mc Graw-Hill, 1° edition.

Koontz, O' Doneel y Weihrich. (2002). **Administración.** México: Mc Graw-Hill.

Kootz, A. y O' Donnel, J. (2000). **Administración.** México: Mc Graw-Hill.

Leonard, William. (2000). **Auditoría Administrativa.** México: Diana.

Martin, C. (2000). **Information Systems. A Management Perspective.** New York: Mc Graw-Hill.

Martin, W. (1994). **Seguridad en Computación.** México: Limusa.

Meyer, Mathias. (2002). **Cryptography.** New Jersey: John Wiley & Son.

Murdic, R. (2001). **Sistemas de Información Administrativa.** México: Prentice-Hall, 2° edición.

Nuevo Diccionario Español *Sopena.* (2002).

Nuevo **Diccionario Español *Sopena***. (2002). España: Espasa-Calpé.

Piattini, M. y del Peso, E. (1998). **Auditoria Informática: Un Enfoque Práctico.** México: Editorial Ra-ma.

Porter, H. (2002). **Computer Audit Guidelines.** Toronto, Canada: Canadian Institute of Chartered Accounts.

Porter, Jr. y Thomas, W. (2001). **Audioria de Sistemas Electrónicos.** México: Editorial Herrero Hermanos, 2° edición.

Rangel Medina, David. (1998). **Derecho Intelectual.** México: Mc Graw-Hill, 1° edición.

Sánchez Curiel, Gabriel. (1997). **Auditoria de Estados Financieros, en Caso Práctico.** México: Mc Graw-Hill.

Schulthers, R. y Sumner, M. (1998). **Management Information System. The Management View.** New York: Mc Graw-Hill.

Secretaría de Gobernación. (2000). **Ley Federal de Derechos de Autor.** México: SEGOB.

Seen, James. (1998). **Information System Management.** Belmont, California: Wadsworth Publishing Company Inc.

Tanenbaum, A. (1997). **Redes de Computación.** México: Prentice-Hall, 3° edición.

Trickner, R. (1996). **Management Information and Control System.** Oxford Center for Management Studies: Willer-Interscience Publication.

Vaquero, Antonio y Jopnes, Luis. (2002). **Informática: Glosario de Términos y Siglas.** México: Mc Graw-Hill.

Weber, Ron. (2001). **Auditing Conceptual Foundations and Practice.** New York: Mc Graw-Hill.

Werss, H. (2002). **The System Development Audit.** New York: PTH International Conference of EDP, Auditor Association.

Willmar, K. (2001). **Information System in Management.** Reston, Virginia: Reston Publishing Company Inc., 1° edition.

ÍNDICE.