TECNOLÓGICO UNIVERSITARIO DE MÉXICO

ESCUELA DE INFORMÁTICA

INCORPORADA A LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
CLAVE 3079-48

“PRINCIPIOS BÁSICOS PARA LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN”

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN INFORMÁTICA

PRESENTA:

SBAIDEE PÉREZ MILÁN

ASESOR DE TESIS:
L.I. JOSÉ FRANCISCO ÁGUILA PATIÑO

MÉXICO, D.F. 2007

AGRADECIMIENTOS

A MIS PADRES

Porque sólo la superación de mis ideales
me han permitido comprender cada día
más la difícil posición de ser padres,
mis conceptos, mis valores morales
y mi superación se las debo a ustedes,
esto será la mejor de las herencias,
lo reconozco y lo agradeceré eternamente.
En adelante pondré en práctica
mis conocimientos y el lugar que en mi mente
ocuparon los libros, ahora será de ustedes,
esto, por todo el tiempo que les robé pensando en mí.

A MI HERMANA

Gracias por tu apoyo y paciencia,
pero sobre todo gracias por creer en mí.

A MI ASESOR DE TESIS
(L.I José Francisco Águila Patiño)

Gracias por su valiosa colaboración y
apoyo en la realización de la presente tesis

GRACIAS
S B A I D E E

“PRINCIPIOS BÁSICOS PARA LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN”

INTRODUCCIÓN

La informática ha evolucionado de forma acelerada en los últimos tiempos, por lo tanto se ha convertido en una parte importante de nuestras vidas, ya que la podemos encontrar en las diferentes actividades cotidianas, es decir en el hogar, el colegio, el trabajo, etc. Debido a que la informática es una disciplina muy amplia, se encuentra dividida en diversas áreas, esto es con el propósito de cubrir los diferentes aspectos de la actividad informática. Una de las áreas de la informática es la auditoría en informática la cual se define como la unión de técnicas, actividades y procesos encaminados a analizar, evaluar y verificar los asuntos relacionados con el servicio informático, con el fin de mejorar la eficiencia, confiabilidad y seguridad de la información.

A su vez la auditoría en informática se divide en cinco grandes ramas, las cuales son: auditoría de explotación, auditoría de desarrollo, auditoría de sistemas de información, auditoría de comunicaciones y auditoría de seguridad. Como podemos ver la auditoría en informática es un tema muy extenso, por lo tanto la presente tesis se enfoca en analizar únicamente la auditoría de sistemas de información con el propósito de dar a conocer los principios básicos para realizar dicha auditoría. Por lo anterior, el objetivo de la presente tesis es proponer una metodología específica para realizar la auditoría de sistemas de información, dicha metodología consta de tres pasos, planeación, ejecución y dictamen de la auditoría. Cabe señalar que la técnica de evaluación de los sistemas de información que expone esta tesis se basa en el ciclo de vida del desarrollo de los mismos, debido a que esta técnica permite evaluar cualquier sistema de información por más complejo que sea.

Después de haber dado a conocer el contenido de mi tesis, es momento de explicar las razones que me llevaron a realizarla. La idea surge en el octavo semestre de mi carrera, ya que en este semestre se impartía la materia de auditoría en informática, en ella aprendí de forma general cada una de las ramas en las que se divide, pero en especial llamo mi atención la auditoría de sistemas de información, por lo tanto decidí realizar mi tesis sobre este tema, esperando que sirva de consulta para posteriores generaciones.

CAPÍTULO 1. INTRODUCCIÓN A LA AUDITORÍA INFORMÁTICA.

1.1 Conceptos generales.

1.1.1 Auditoría, informática y sistema de información.

Auditoría. La palabra Auditoría se ha considerado incorrectamente como una evaluación cuyo único fin es detectar errores y señalar fallas. Por lo tanto se cree que la auditoría surge de un error o una falla, es decir, solamente se realiza cuando se han detectado errores.

Echenique García, José Antonio[1] define auditoría como:
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 logar los objetivos propuestos.

La palabra Auditoría viene del latín “auditorius”, y de ésta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír. Por otra parte, el diccionario Español Sopena lo define como revisor de cuentas colegiado. Por lo anterior, el auditor al tener la virtud de oír y revisar cuentas, debe establecer y seguir un objetivo especifico, el cual es la evaluación de la eficiencia y la eficacia con que se está operando, con el fin de corregir los errores, en caso de que existan, mediante cursos alternativos de acción que permitan la toma de decisiones.

Hernández García, Alonso[2] define y divide la auditoría de la siguiente manera:
Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Podemos descomponer este concepto en los elementos fundamentales que a continuación se especifican:

[1] Echenique García, José Antonio, Auditoría en informática, editorial Mc Graw Hill.

[2] Piattini, Mario G, y Emilio del Peso, Auditoría informática, editorial Alfaomega-Rama.

1. *Contenido: Una opinión.*
2. *Condición: Profesional.*
3. *Justificación: Basada en determinados métodos.*
4. *Objeto: Una determinada información obtenida en un cierto soporte.*
5. *Finalidad: Determinar la fiabilidad de la realidad.*

Podemos definir el concepto de auditoría como una evaluación estricta y sistemática de la eficiencia y eficacia de determinada área u organismo, con el fin de determinar la fiabilidad y veracidad de la información, además, en caso necesario dotará a la organización de las herramientas necesarias que le permitan mejorar y lograr sus objetivos.

Informática. La palabra Informática proviene del vocablo francés informatique, el cual forma a su vez las palabras información y automatique, que quiere decir información automatizada.

Beekman, George[3] define informática como:
Ciencia que se ocupa del tratamiento de la información, utilizando medios automáticos.

La Academia Francesa reconoció el concepto de informática en el año de 1966 y lo definió de la siguiente manera: *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.*

Más tarde en el año de 1975 la Oficina Intergubernamental de Informática (IBI), órgano asociado a la UNESCO, proporciono una nueva definición de informática debido a las limitaciones que presentaba la definición otorgada por la Academia Francesa.

La definió como: *Aplicación racional, sistemática de la información para el desarrollo económico, social y político.*

[3] Beekman, George, Computación & Informática Hoy, editorial Iberoamericana.

Dos años después La Academia Mexicana de Informática en el año de 1977 intentó renovar y mejorar el concepto de informática proponiendo la siguiente definición: *Ciencia de los sistemas inteligentes de información*.

Así podemos darnos cuenta que el concepto de informática tiene un sentido más extenso y abarca 3 puntos importantes:

- Considera el sistema en su totalidad.
- Manejo de la información y,
- Hardware.

Por lo tanto el concepto de informática se puede definir como el conjunto de conocimientos científicos y técnicas que consideran el sistema en su totalidad haciendo posible el tratamiento automático de la información por medio de ordenadores.

Sistema. Nuestra vida está rodeada de sistemas, podemos comenzar mencionando el sistema más grande y maravilloso, el cuerpo humano, el cual formado por el sistema nervioso, circulatorio, respiratorio, digestivo, etc., logra realizar todas las funciones del ser humano. También podemos mencionar otros tipos de sistemas como el económico, político y social. En informática, la palabra sistema es utilizada con diversos sentidos, por ejemplo si hablamos de una computadora el sistema está formado por hardware y su sistema operativo.

Seen, James[4], define sistema como:
En el sentido más amplio, un sistema es un conjunto de componentes que interaccionan entre sí para lograr un objetivo común.

Por ejemplo un hospital es un sistema y sus componentes son las diversas especialidades, laboratorio, quirófano, urgencias, personal, entre otras. Así cada uno de los componentes es un sistema, por ejemplo el área de especialidades está formada

[4] Seen, James, Análisis y diseño de Sistemas de Información, editorial Mc Graw Hill.

por cardiología, otorrinolaringología, ginecología, etc., y a su vez trabajan en equipo con el fin de obtener ganancias en beneficio común.

Sistema de información. Es el medio por el cual los datos fluyen de una persona o departamento hacia otros, por ejemplo un sistema de cómputo que genera reportes de forma periódica para varios usuarios. Los sistemas de información son los responsables de brindar servicio a todos los sistemas de la organización y de unir todos los componentes de ésta con el fin de lograr que trabajen con eficiencia y logren los objetivos establecidos.

1.1.2 Auditoría en informática y auditoría de sistemas de información.

Auditoría informática. La informática tiene gran importancia en el funcionamiento de una empresa ya que participa en la gestión y toma de decisiones de la misma, por lo anterior existe la auditoría en informática.

Rivas, Gonzalo Alonso[5] define la auditoría informática como:
La auditoría informática es un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio, o del sistema, que resultan auditados.

En está definición hay cuatro palabras que destacan sobremanera: examen, metódico, puntual, discontinuo. Esta relevancia podría justificarse diciendo que la auditoría informática es un examen, pues debe partir de una situación dada; que éste es metódico, puesto que seguirá un plan de trabajo perfectamente sistematizado que permita llegar a conclusiones suficientemente fundamentadas (conclusión ésta exigible a cualquier auditoría); que es puntual; ya que se da un corte en el calendario para llevarla a cabo, y que es discontinua , extraña a servicio de informática, en aras de

[5] Rivas, Gonzalo Alonso, Auditoría informática, Ediciones DÍAZ DE SANTOS, S.A.

buscar la objetividad requerida, por lo cual será ejecutada por personas ajenas al departamento independientes de las funciones a auditar.

Podemos definir el concepto de auditoría en informática como la unión de técnicas, actividades y procesos encaminados a analizar, evaluar y verificar los asuntos relacionados con el servicio informático, con el fin de mejorar la eficiencia, confiabilidad y seguridad de la información.

Un punto importante es la información organizacional ya que participa en la toma de decisiones, por ejemplo si un sistema reporta datos desacertados esto traerá como consecuencia una grave y errónea toma de decisiones y por lo tanto se verá afectada la organización. A continuación se mencionan las principales causas que incitan la realización de la auditoría informática. Véase Tabla 1.

PRINCIPALES CAUSAS DE LA AUDITORÍA INFORMÁTICA	
Abuso de los ordenadores.	Perder información de manera intencional o con el fin de obtener alguna utilidad.
Abuso del personal.	Realizar trabajos que no tienen que ver con la organización así como hacer uso indebido de los recursos informáticos de la misma.
Errores u omisiones.	Estas causan perdidas a la organización.
Causas naturales.	Se refiere a incendios, suministro de energía.
Insatisfacción de los usuarios.	No se atienden las peticiones de los usuarios.
Debilidades económico-financieras.	Incremento desmesurado de costos.
Inseguridad.	El nivel de riesgo es alto.

Tabla 1. Principales causas de auditoría informática.

La auditoría en informática no solo debe enfocarse a los equipos, sistemas y procedimientos, sino también en evaluar los *sistemas de información* en general, es decir, entradas, flujo de información, proceso, salida, archivos, respaldos, controles, confidencialidad, seguridad y personal. Así la auditoría en informática debe tomar en cuenta todo el entorno informático ya que cada una de las áreas que conforman a la informática es de fundamental importancia para el desarrollo organizacional.

Auditoría de sistemas de información. Actualmente los sistemas se han convertido en la herramienta con más poder para materializar el concepto más trascendente y necesario en cualquier organización, los sistemas de información. A continuación se mencionan algunos conceptos de auditoria de sistemas de información. Véase Tabla 2.

CONCEPTOS AUDITORÍA DE SISTEMAS DE INFORMACIÓN
La verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad y presentar recomendaciones a la Gerencia.
La actividad dirigida a verificar y juzgar información.
El examen y evaluación de los procesos del Área de Procesamiento automático de Datos (PAD) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas.
Es el examen o revisión de carácter objetivo (independiente), crítico(evidencia), sistemático (normas), selectivo (muestras) de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, con el fin de emitir una opinión profesional.

Tabla 2. Conceptos auditoría de sistemas de información.

La auditoría de sistemas de información se puede definir como la técnica que abarca de forma general o particular la revisión y evaluación de todos los aspectos relacionados con los sistemas automatizados de procesamiento de la información.

La importancia de este tipo de auditoría radica en optimizar el buen desempeño de los sistemas de información, ya que esta proporciona los controles necesarios que permiten a los sistemas ser confiables y gozar de un alto nivel de seguridad.

1.1.3 Tipos de auditoría en informática.

Tipos de auditoría informática. De forma general la auditoría informática se divide en dos tipos: auditoría operativa y auditoría funcional, estas a su vez se dividen en: auditoría de gestión, auditoría de procedimientos y auditoría de cifras. A continuación se muestra de forma gráfica los tipos de auditoría informática. Véase Ilustración 1.

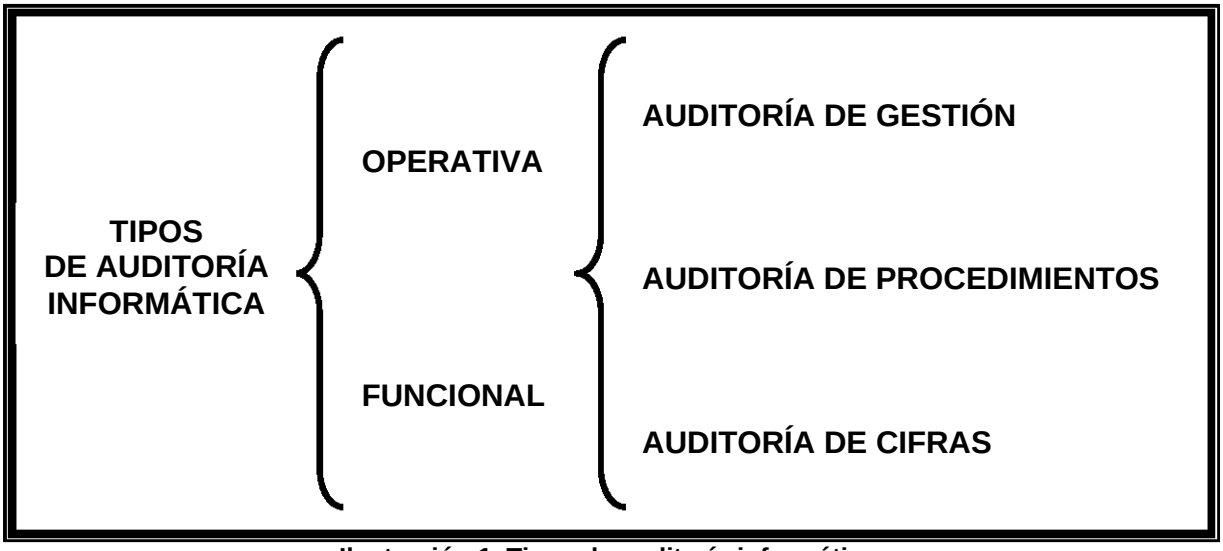

Ilustración 1. Tipos de auditoría informática.

Auditoría informática operativa. Este tipo de auditoría se enfoca en evaluar las actividades que engloban a uno o varios servicios, además, requiere de la realización exhaustiva de un examen con el fin de restaurar los errores que se encuentren al final de dicha evaluación. Dentro del entorno de la auditoría informática operativa los siguientes 3 tipos de auditoría se desarrollan de la siguiente manera:

Auditoría de gestión.

- Estudia los gastos y la eficacia de la aplicación evaluada.
- Vigila el correcto funcionamiento de la planeación de proyectos.

- Establece los controles utilizados en la realización de un proyecto enfocándose en los controles internos utilizados en la gestión de proyectos.
- Evalúa la calidad y utilidad de la información arrojada por el sistema, así como el beneficio económico del proyecto.

Auditoría de procedimientos.

- Se encarga de asegurar que las normas y procedimientos se cumplan de forma total.
- Deberá cerciorarse que tales normas y procedimientos para la gestión existan así como verificar su adecuado establecimiento.
- Evaluará si las normas y procedimientos son tomados en cuenta por el personal informático y usuarios.
- La auditoría de procedimientos esta facultada para emitir juicios de valor respecto a los procedimientos y normas auditados, generalmente estas normas se refieren al mantenimiento de las aplicaciones, mediante la evaluación de los controles.

Auditoría de las cifras.

- Protege el establecimiento de controles para asegurar el buen funcionamiento de los datos, es decir, su exactitud y calidad, además, trata de impedir fraudes.
- Estos controles no se emplearán solamente en las áreas informáticas también se llevarán acabo en las áreas de proveedores y consumidores de datos ya que el problema puede surgir de estas.

Auditoría informática funcional. Este tipo de auditoría evalúa el funcionamiento de las actividades informáticas de una o varias unidades perfectamente definidas. La auditoría informática funcional realizará un juicio del buen funcionamiento de la función informática, además, juzgará su eficiente establecimiento dentro de la estructura general de la organización. Dentro del entorno de la auditoría informática funcional los siguientes tipos de auditoría se desarrollan de la siguiente manera. Véase Tabla 3.

AUDITORÍA DE GESTIÓN	AUDITORÍA DE PROCEDIMIENTOS
— Este tipo de auditoría abarca todo aquello que sea capaz de evaluar el nivel de integración de la informática en la empresa.	Evalúa los componentes más notorios como son: — La seguridad del local en donde se encuentra ubicado el centro de proceso de datos (esta evaluación es a nivel hardware-software). — Procesos de explotación. — Establecimiento de normas de trabajo lo más reducidas que se pueda así como el cumplimiento de las mismas. — Seguridad de las aplicaciones etc.

Tabla 3. Auditoría de gestión y procedimientos.

En conclusión la auditoría informática funcional evalúa todos los aspectos referentes a la función informática con el fin de convertir ha esta en un instrumento eficiente al servicio de la gestión y que permita justificar los gastos elevados realizados con el fin de obtener o adquirir un(os) bien(es) o servicio(s) intentando minimizar los gastos a costa de reducir su implantación.

1.2 Áreas y campo de acción de la auditoría en informática.

Áreas de la auditoría informática. Comenzaremos mencionando las seis áreas de aplicación de la auditoría informática propuestas por Rivas, Gonzalo Alonso[6].

- *Planificación: donde se pasa revista a las distintas fases de la planificación.*
- *Organización y administración: Aquí se examinarán aspectos como las relaciones con los usuarios, con los proveedores, asignación de recursos, procedimientos, etc.*

[6] Rivas, Gonzalo Alonso, Auditoría informática, Ediciones DÍAZ DE SANTOS, S.A.

- *Construcción de sistemas: área importante donde la auditoría velará por la adecuación de la informática a las necesidades reales de la empresa. Labor que no siempre es fácil.*
- *Explotación: aquí se analizarán los procedimientos de operación y explotación en el centro de procesos de datos.*
- *Entorno hardware: donde se vigilará, entre otras cosas los locales del Centro de Procesamiento de Datos., el acceso a éstos, alarmas, sistemas anti-incendios, protección de los sistemas, fiabilidad del hardware, etc.*
- *Entorno software: en esta área la auditoría informática analizará los sistemas de prevención y detección de fraudes, los exámenes a aplicaciones concretas, los controles a establecer…, en definitiva, todo lo relacionado con la fiabilidad, integridad y seguridad del software.*

El siguiente cuadro muestra una clasificación más completa respecto a las áreas de la auditoría informática. Véase Ilustración 2.

ÁREAS ESPECIFICAS	ÁREAS GENERALES			
	INTERNA	DIRECCION	USUARIO	SEGURIDAD
De Explotación				
De Desarrollo				
DE SISTEMAS				
De Comunicaciones				
De Seguridad				

Ilustración 2. Áreas de la auditoría informática.

Comenzaremos explicando las áreas generales de la auditoría informática:

- Auditoría informática de actividades internas. Este tipo de auditoría se enfoca en la informática interna, es decir, en las actividades que lleva acabo la informática de forma real y cotidiana.
- Auditoría informática de dirección. Su importancia de este tipo de auditoría radica en la capacidad que posee para interpretar las necesidades de la organización. Su objetivo es controlar la función del área informática con el usuario, es decir, evaluar las relaciones entre ellas.
- Auditoría informática de usuario. Este tipo de auditoría maneja el exterior es decir, al usuario, debido a que el área informática dirige sus actividades hacia el.
- Auditoría informática de seguridad. Este tipo de auditoría se ocupa de evaluar los niveles de riesgo a los que esta expuesta la organización.

Dentro de las áreas generales, se encuentran las áreas específicas estas pueden ser auditadas usando los criterios generales: Las áreas específicas son:

- Auditoría informática de explotación. La explotación informática tiene como fin producir resultados informáticos de cualquier tipo, para ello necesita “datos” los cuales serán transformados a través de un proceso informático “programas”, con el fin de obtener un resultado, el cual será entregado al usuario. La auditoría de explotación se encarga de auditar las siguientes áreas: planificación, producción y soporte técnico, evaluándolas de forma individual y tomando en cuenta sus interrelaciones.

- Auditoría informática de desarrollo de proyectos. La auditoría informática de desarrollo es conocida como la evaluación del análisis, desarrollo de sistemas y aplicaciones. De forma general una aplicación se compone por: prerrequisitos (del usuario y entorno), análisis de funcionalidad, diseño, análisis de la preprogramación y programación, realización de pruebas, entregar a explotación y realizar alta para el proceso. Los puntos mencionados anteriormente se someterán a control interno y tomarán en cuenta los costes y que podría existir

insatisfacción del usuario, además, comprobará que los programas ejecutados por la maquina sean los correctos.

- Auditoría informática de sistemas. La auditoría de sistemas se encarga de evaluar la técnica de sistemas en todas sus etapas.
- Auditoría informática de comunicaciones. Este tipo de auditoría analizará todo lo referente a las comunicaciones, líneas y redes.
- Auditoría informática de seguridad**.** Este tipo de auditoría se encarga de estudiar los riesgos a los que se enfrenta la organización. La seguridad informática se divide en: física y lógica, la seguridad física protege el hardware y los soportes de datos así como las instalaciones en donde se encuentran, abarca robos incendios, etc. Mientras que la seguridad lógica evalúa el uso de software, protege los datos, procesos y programas, acceso a la información etc.

Campo de acción de la auditoría informática. Ahora ya conocemos las diferentes áreas de la auditoría informática, por lo tanto es momento de conocer el campo de acción de esta. Echenique García, José Antonio[7] nos dice que el campo de la auditoría en informática es:

- 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 (software, hardware, redes, bases de datos, comunicaciones).
- Seguridad y confidencialidad de la información.
- Aspectos legales de los sistemas y de la información.

Asimismo desglosa cada uno de los campos anteriores:

A) Evaluación administrativa del departamento de informática. Esto comprende la evaluación de:

[7] Echenique García, José Antonio, Auditoría en informática, editorial Mc Graw Hill.

— 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 pueden 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 en la utilización de los equipos.
- Plan de contingencia y procedimiento de respaldo para casos de desastre.
- Restauración de equipo y de sistemas.

1.3 Objetivos de la auditoría en informática.

Comenzaremos mencionando el objetivo principal de la auditoría informática según Yann, Derrien[8]. *El objetivo principal de una auditoría informática es siempre el mismo: comprobar la fiabilidad de la herramienta informática y la utilización que se hace de la misma.* A continuación se mencionará la clasificación propuesta por el autor respecto a los objetivos de la auditoría informática. Los objetivos son:

- Examinar la fiabilidad del ambiente informático.
- Examinar la eficacia y la forma de actuar de la actividad informática.
- Examinar la fiabilidad de una aplicación informatizada.
- Utilizar la herramienta informática en una misión de auditoría.

[8] Yann, Derrien, Técnicas de la auditoría informática, editorial Alfa-omega.

Ahora que conocemos los objetivos de la auditoría informática propuestos por Yann, Derrien, nos enfocaremos en desarrollar una clasificación propia de estos tomando en cuenta que la auditoría informática tiene como propósito mantener el buen funcionamiento del entorno informático. Los objetivos de la auditoría informática son: Véase Ilustración 3.

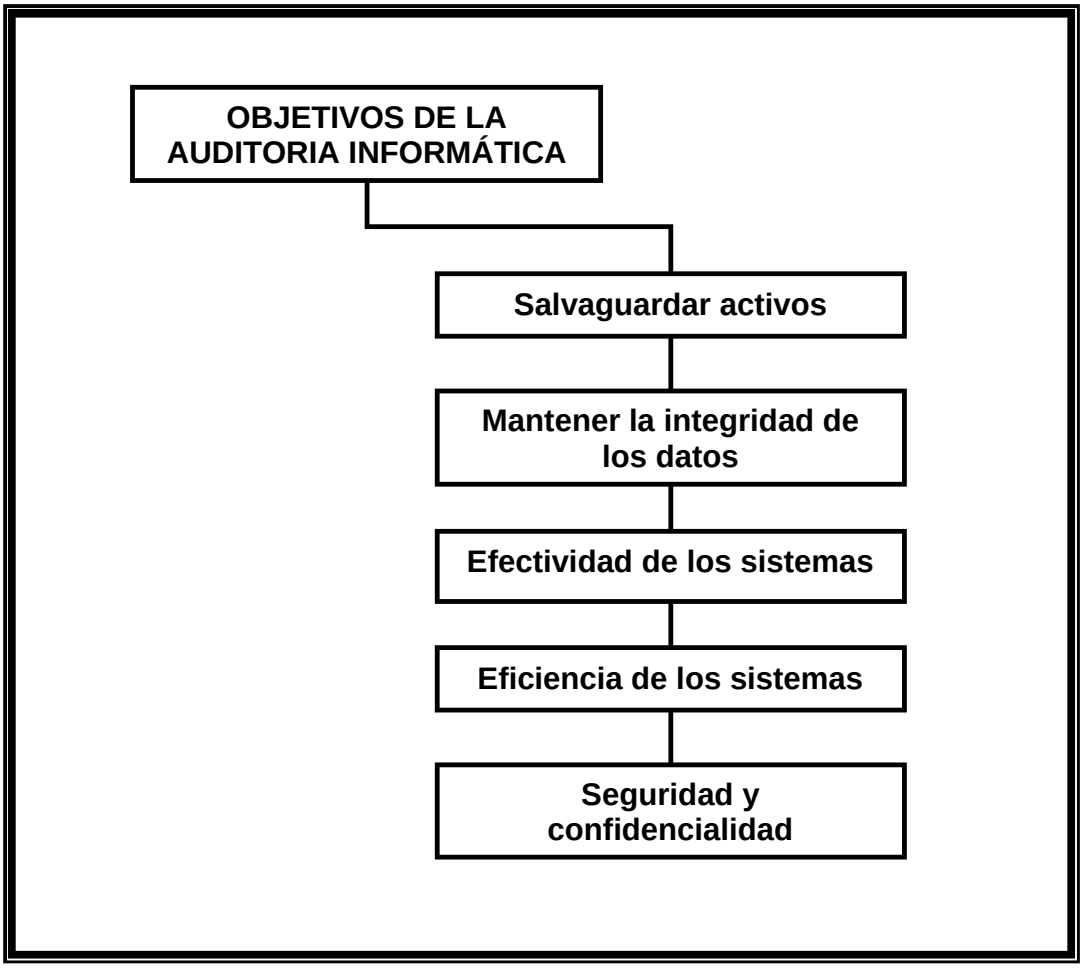

Ilustración 3. Objetivos de la auditoría informática.

A continuación se explicarán cada uno de los objetivos de la auditoría informática que aparecen en la ilustración anterior.

- Salvaguardar activos. Se protege el hardware, software y recursos humanos de la organización.
- Mantener la integridad de los datos. Esta garantiza que la información es modificada, creada y borrada, solo por el personal autorizado.

- Efectividad de los sistemas. Se refiere a la capacidad que tiene un sistema para cumplir con los objetivos de la organización.
- Eficiencia de los sistemas. Se refiere a la capacidad que tiene un sistema para cumplir los objetivos con los menores recursos.
- Seguridad y confidencialidad. La primera busca la protección contra los riesgos aliados a la informática tales como la vulnerabilidad y amenazas de los activos, mientras que la segunda se encarga de asegurar que la información no este disponible o que esta no sea descubierta por personas, entidades o procesos no autorizados.

Cabe mencionar que los objetivos de la auditoría informática solo se podrán alcanzar si la administración de la organización logra desarrollar un adecuado control interno.

1.4 Control interno informático.

Control interno informático. Se define como el órgano de la dirección del departamento de informática encargado de controlar diariamente que todas las actividades de los sistemas de información se realicen cumpliendo con las normas estándares y procedimientos establecidos por la organización, así como los requerimientos legales.

Objetivos del control interno informático. Los objetivos específicos del control interno informático según Muñoz Razo, Carlos[9] son:

- *Establecer como prioridad la seguridad y protección de la información, del sistema computacional y recursos informáticos de la empresa.*
- *Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.*
- *Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.*

[9] Muñoz Razo, Carlos, Auditoría en sistemas computacionales, editorial Pearson Education.

— *Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.*

— *Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa.*

Elementos del control interno informático. La siguiente ilustración muestra los elementos del control interno informático aplicables en el área de sistemas. Véase Ilustración 4.

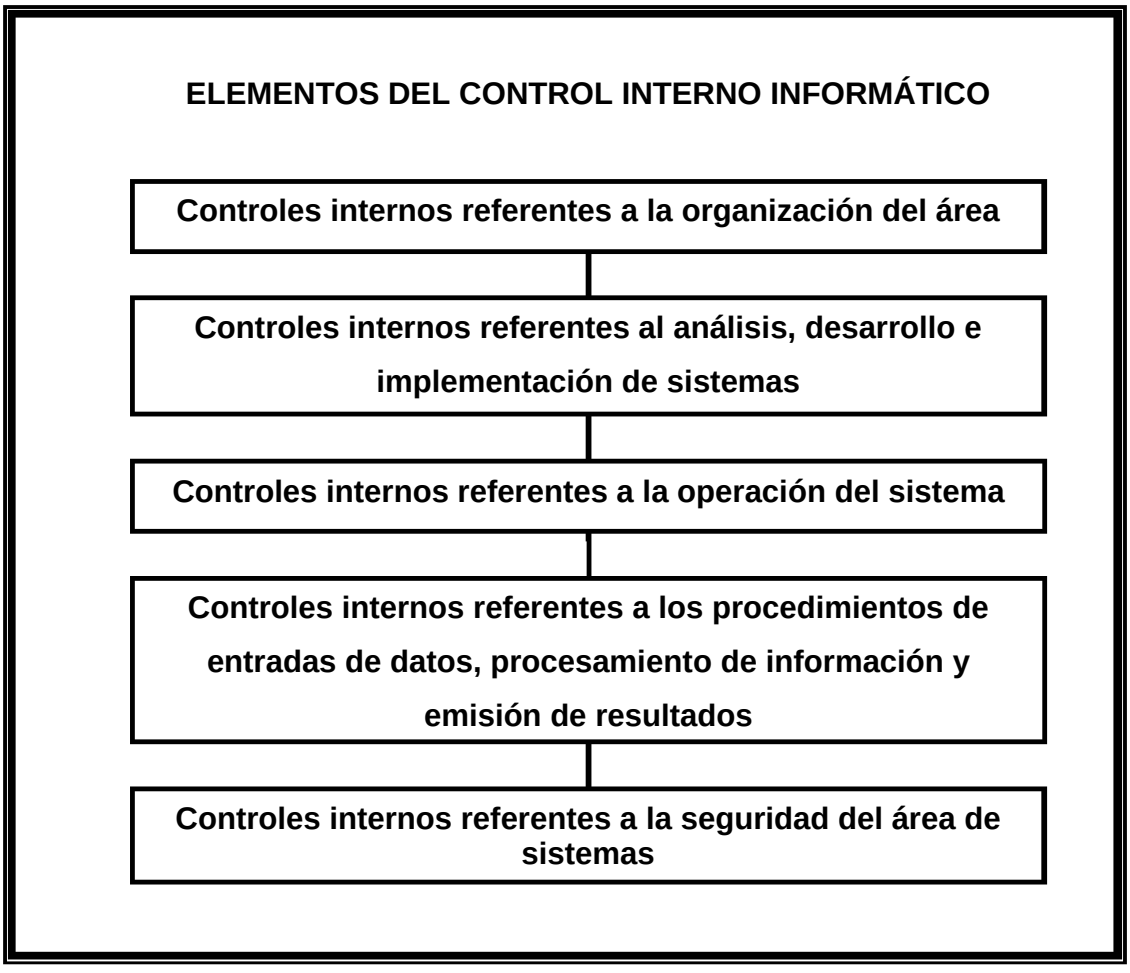

Ilustración 4. Elementos del control interno informático.

A continuación se detallarán cada uno de los elementos mencionados en la ilustración anterior.

Controles internos referentes a la organización del área:

- Dirección.
- División del trabajo.
- Nombramiento de responsabilidad y autoridad.
- Establecer estándares y métodos.
- Perfil de puestos.

Controles internos referentes al análisis, desarrollo e implementación de sistemas:

- Estandarizar las metodologías para el desarrollo de proyectos.
- Garantizar que el beneficio del sistema sea sumamente bueno.
- Realizar estudios de factibilidad del sistema.
- Asegurar la eficiencia y la eficacia en la etapa de análisis y diseño de sistemas.
- En la etapa de implantación y mantenimiento del sistema se deberá cuidar la efectividad y eficacia de los sistemas.

Controles internos referentes a la operación del sistema.

- Los errores de operación se deberán prevenir y en determinado caso corregir.
- Prevenir y evitar el mal uso de la información.
- Aplicar medidas para mantener la seguridad en la información.
- Conservar la confiabilidad, oportunidad, veracidad y capacidad en el procesamiento de la información de la organización.

Controles internos referentes a los procedimientos de entradas de datos, procesamiento de información y emisión de resultados:

- Checar la existencia y función de los procesos de captura de datos.
- Verificar que los datos introducidos sean procesados correctamente.
- Verificar que los resultados arrojados mediante el procesamiento de información sean oportunos, confiables y veraces.

- Comprobar que el procesamiento de datos sea confiable, veraz y exacto.

Controles internos referentes a la seguridad del área de sistemas:

- Prevenir amenazas, riesgos y contingencias en las áreas sistematizadas.
- Seguridad física del área de sistemas.
- Seguridad lógica de los sistemas.
- Seguridad de la base de datos.
- Controlar la operación de los sistemas.
- Seguridad del personal de informática.
- Seguridad de la telecomunicación de datos.
- Seguridad de redes y sistemas multiusuarios.

De esta forma podemos concluir que el control interno informático es una actividad que tiene como fin prevenir y corregir irregularidades que puedan afectar el buen funcionamiento de un sistema para lograr sus objetivos.

1.5 Importancia de la auditoría en informática.

De manera general la auditoría informática es importante debido a que permite expresar juicios objetivos apoyándose de la evaluación realizada de las debilidades y aciertos del entorno informático.

¿Por qué es importante la auditoría informática?

- Participa en la toma de decisiones de la organización.
- Evalúa la adecuada utilización de los sistemas de información.
- Permite mejorar la operatividad organizacional.
- Controla el uso de la computadora debido a su importancia y costo.
- Control de personal.
- Controla el abuso de las computadoras.

- Corrige y mejora los sistemas de información que lo necesitan con el fin de optimizarlos.
- Controla la información (mal uso o duplicidad).
- Mantiene la privacidad de la organización.

Ahora que ya hemos conocido el entorno global de la auditoría informática es momento de enfocarnos en el objeto de estudio de la presente tesis titulada “Principios básicos para la auditoría de sistemas de información” por lo que en el siguiente capítulo se realizará un análisis sobre la planeación de la auditoría de sistemas de información.

CAPÍTULO 2. PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN.

2.1 Planeación.

Planeación. Es el proceso de decidir de antemano qué se hará y de qué manera. Incluye determinar la misión global, identificar los resultados clave y fijar objetivos específicos, así como políticas para el desarrollo, programas y procedimientos para alcanzarlos[10].

La planeación es un paso muy importante en la auditoría de sistemas de información ya que de esta depende lograr una auditoría eficiente, por lo tanto una mala planeación tendrá como resultado diversos problemas como impedir su cumplimiento o que se efectúe sin el debido profesionalismo. A continuación se mencionarán las etapas de la planeación de la auditoría de sistemas. Véase Ilustración 5.

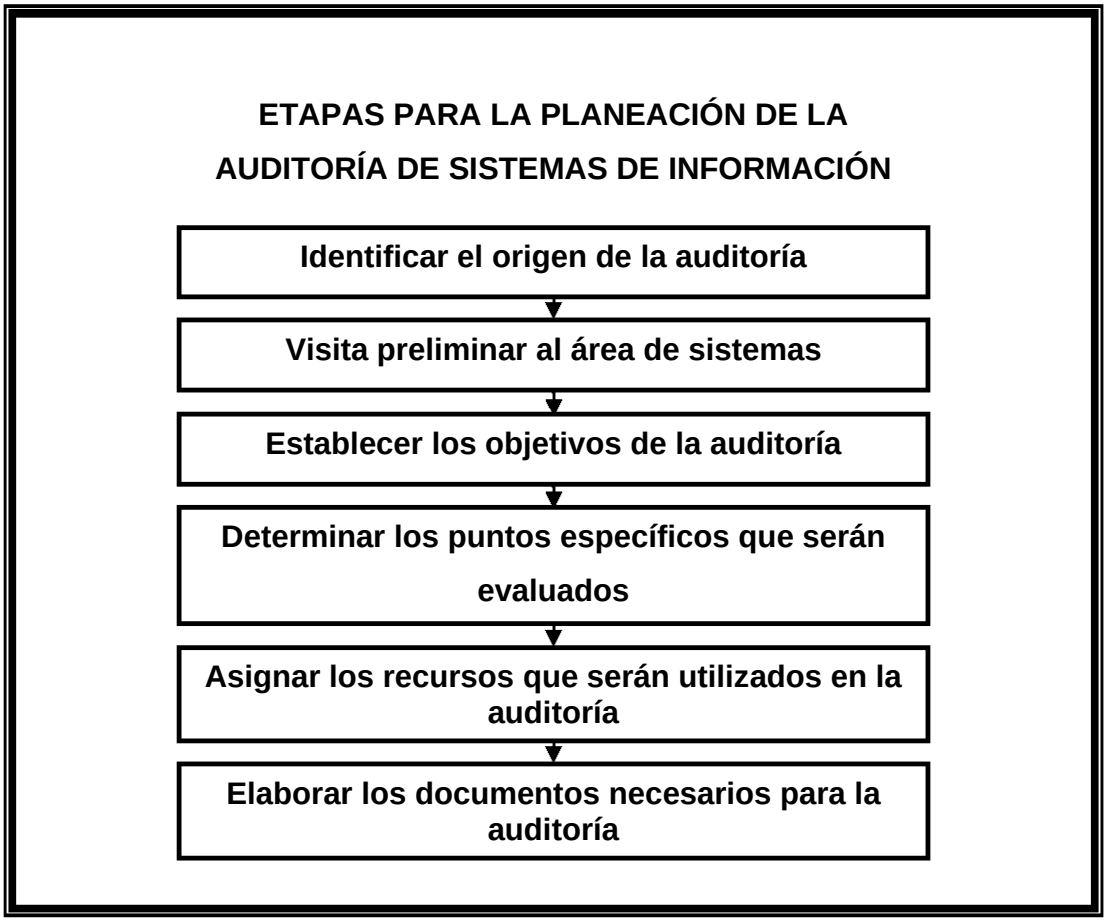

Ilustración 1. Etapas para la planeación de la auditoría de sistemas de información.

[10] Muñoz Razo, Carlos, Auditoría en sistemas computacionales, editorial Pearson Education.

En los siguientes puntos se detallarán cada una de las etapas para la planeación de la auditoría de sistemas de información que muestra la ilustración anterior.

2.2 Etapas de la planeación.

2.2.1 Identificar el origen de la auditoría.

El primer paso de la planeación es conocer como surge la necesidad de realizar una auditoría por lo tanto debemos preguntarnos ¿de dónde?, ¿por qué?, ¿quién? o para qué se necesita realizar una evaluación de algún aspecto de los sistemas de la organización. Es importante para el auditor identificar el origen de la auditoría debido a que:

- Proporciona los elementos para llevar acabo una buena planeación de la revisión.
- Ayuda a definir los elementos de juicio que contribuirán a dictar las normas que regirán su criterio de evaluación.
- Define la forma en la que dirigirá la revisión.
- Identifica los asuntos sobre los que deberá trabajar con el propósito de satisfacer lo que se espera de la auditoría.

El origen de la auditoría podría ser ocasionado por los siguientes puntos:

Por solicitud expresa de procedencia interna. La evaluación surge debido a una petición formal realizada por alguien que pertenece a la organización. Esta petición puede ser originada por muchas causas, por lo tanto la evaluación puede llevarse acabo por un auditor externo o por un auditor interno.

De esta petición se derivan los siguientes orígenes internos:

- Por petición de accionistas, socios y dueños de la organización. Esta petición de auditoría es considerada como una orden debido a su origen y es generalmente

realizada por auditores externos con la finalidad de contar con un criterio más objetivo respecto el aprovechamiento de los sistemas.

- Por orden de la dirección general. Esta petición es realizada por la máxima autoridad de la organización por lo tanto es irrevocable. Las causas que la originan pueden ser evaluar periódicamente al área de sistemas, verificar la forma de actuar de los dirigentes del área, por desconfianza, entre otras, por lo tanto el auditor deberá establecer los motivos reales de la auditoría con la finalidad de enfocar sus acciones en satisfacer estos.
- Por solicitud de las gerencias. Esta petición es realizada por la gerencia o departamentos de mando superior en la organización, la auditoría puede o no realizarse, esto dependerá del nivel de importancia que esta presente para la organización.
- Por solicitud de funcionarios y empleados. El origen de esta petición de auditoría no es común debido a que surge de los niveles más bajos de la organización, por lo tanto, los mandos superiores deberán analizar la petición y de esta forma decidir si se aprueba o no.

Por solicitud expresa de procedencia externa. La evaluación surge debido a una petición formal realizada por alguien ajeno a la organización, a quien, por algún motivo, le interesa que sean auditados los sistemas de está.

De esta petición se derivan los siguientes orígenes externos.

- Por mandato de autoridades judiciales. Esta petición de auditoría es de carácter obligatorio. Algunas de las causas que originan esta auditoría son: auditorias anteriores, petición de terceros, piratería, carencia de licencias para el uso de software, mal uso del software, mal uso de la información de los sistemas, delitos informáticos entre otros.
- Por orden de las autoridades fiscales. Las autoridades fiscales imponen la realización de la auditoría y por lo tanto deben especificar todos los aspectos que requieren evaluar. Generalmente se lleva acabo con el fin de evaluar la información sistematizada de la empresa.

Por emergencias y condiciones especiales. Esta petición se da cuando se presentan situaciones de emergencia en el área de sistemas por lo tanto se realiza casi de inmediato y por lo general sin autorización de los funcionarios, esta deberá valorar y medir las consecuencias de dichas emergencias con el fin de evaluar el impacto provocado.

Por riesgos y contingencias informáticas. Esta petición es realizada por funcionarios, personal o usuarios del área de sistemas cuando ocurre alguna contingencia de carácter informático que afecte el procesamiento de la información o algún riesgo que pueda influir en las actividades y funciones del área. Por tal motivo se deben evaluar mediante una auditoría de sistemas las consecuencias de cualquiera de estas incidencias. A continuación se muestran los riesgos y contingencias informáticas más comunes:

- Riesgos y contingencias del personal informático.
- Riesgos y contingencias físicas y operativas.
- Riesgos y contingencias de software y de las bases de datos.

Como resultado de los planes de contingencia. Esta solicitud de auditoría en el área de sistemas es propiciada por los planes de contingencia, es decir, si el área de sistemas no cuenta con planes, programas y medidas preventivas de seguridad, esta solicitud ayudará a valorar la necesidad de establecerlos. De lo contrario si el área de sistemas cuenta con planes de contingencia entonces se evaluará su funcionalidad y utilidad para dichos sistemas.

Por resultados obtenidos de otras auditorias. Esta solicitud generalmente se propicia cuando se realiza una auditoría y de esta surge algún aspecto que necesita ser evaluado de forma específica, es decir, el origen de esta auditoría se debe a los resultados de una auditoría anterior.

Como parte del programa global de auditoría. En este tipo de auditoría no existe una solicitud, sino que la auditoría es una disposición concreta de la organización, es decir, surge debido a una evaluación integral de esta.

2.2.2 Visita preliminar al área de sistemas.

Visita preliminar al área de sistemas. Después de haber identificado el origen de la auditoría el siguiente paso que llevará a cabo el auditor será realizar una visita al área de sistemas con el fin de conocer la problemática a la cual se enfrentará por lo tanto comenzará dicha visita relacionándose con el personal e identificará las características principales del área haciéndose las siguientes preguntas:

- ¿Cómo se encuentran distribuidos los sistemas en el área?
- ¿Cuántos, cuáles, cómo y de qué tipo son los equipos que se encuentran instalados en el centro de sistemas?
- ¿Cuáles son las principales características físicas de los sistemas que serán auditados a simple vista?
- ¿Qué tipo de instalaciones y conexiones físicas existen en el área de sistemas?
- ¿Cómo reacciona el personal con la visita del auditor?
- ¿Cuáles son las limitaciones que se observan para llevar acabo la auditoría?

Además, con el fin de analizar y dimensionar el área de sistemas el auditor deberá solicitar la siguiente documentación:

- 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.
- Bases de datos, propietarios de la información y usuarios de la misma.

Por lo tanto el auditor debe tomar en cuenta los siguientes puntos en dicha visita. Véase ilustración 6.

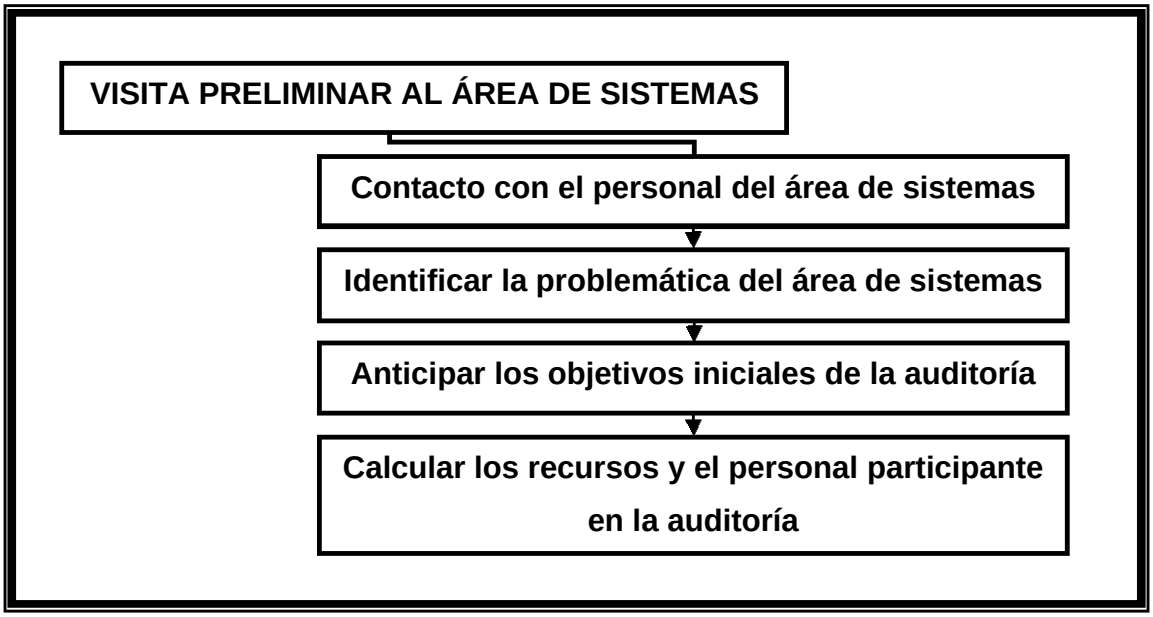

Ilustración 2. Puntos que el auditor deberá tomar en cuenta para realizar la visita preliminar.

A continuación se detallarán los puntos mencionados en la ilustración anterior.

Contacto con el personal del área de sistemas. El auditor realiza una visita preliminar al área de sistemas con el fin de relacionarse con los funcionarios, empleados y usuarios de dicha área con el objeto de medir el nivel de cooperación del personal así como observar la reacción de este ante la realización de una auditoría.

Generalmente el auditor no es bien recibido en área auditada debido a que se cree que la auditoría se está realizando porque se han encontrado errores o para encontrar errores y a los creadores de estos, por la tanto esta idea genera una actitud negativa por parte del personal debido al miedo de perder su empleo, logrando que este se ponga a la defensiva, que no participe en la auditoría, que evada al auditor, que no proporcione la información adecuada, entre otras, es decir los empleados se sienten culpables desde el momento en que se enteran que se llevará acabo una auditoría, aunque no sean responsables de ningún problema que se llegue a detectar.

Así el auditor deberá realizar su visita preliminar en un ambiente de cordialidad pero sin perder su autoridad, pretendiendo con ello tener una buena relación con el personal antes de llevar acabo la evaluación y de esta forma lograr la cooperación del personal.

Por lo tanto podemos concluir que el auditor realiza una visita preliminar al área de sistemas con la finalidad de conocer el ambiente al cual se enfrentará, además, está visita preliminar le servirá para diseñar su estrategia de evaluación la cual tomará en cuenta las expectativas de los funcionarios empleados y usuarios.

Identificar la problemática del área de sistemas. En esta etapa de la visita preliminar el auditor deberá enfocarse en investigar los problemas que enfrentan el área de sistemas, el personal y los usuarios, su procesamiento de información y la administración de sus bases de datos entre otros aspectos. Lo que pretende el auditor con esta investigación preliminar es identificar las posibles dificultades que hay en los sistemas de la organización, por lo que deberá obtener un panorama general de dichas dificultadas aunque estas no sean muy confiables.

Anticipar los objetivos iniciales de la auditoría. Además de lo anterior, el auditor busca mediante la visita preliminar al área de sistemas anticipar que objetivos se podrán cumplir con la auditoría y trata de entender cuales son las metas que se quieren alcanzar con la evaluación. Los objetivos iniciales no son confiables y podrían llevar al auditor por otro camino desviándolo así de los verdaderos objetivos (lo anterior depende de la habilidad, experiencia y conocimientos del auditor) pero estos le ayudarán a establecer su criterio respecto al objetivo que pretende alcanzar con dicha auditoría.

Calcular los recursos y el personal participante en la auditoría. Otro punto importante de la visita preliminar al área de sistemas es calcular el tipo y el número de recursos que se necesitarán para realizar la evaluación tomando en cuenta los siguientes recursos:

- Recursos humanos.
- Recursos informáticos.
- Recursos materiales.
- Recursos técnicos.
- Recursos económicos.

2.2.3 Establecer los objetivos de la auditoría.

Después de haber visitado el área de sistemas el auditor deberá enfocarse en establecer de forma clara el objetivo o los objetivos de la auditoría procurando que estos se acoplen con las necesidades de dicha auditoría, es decir, en esta etapa el auditor deberá realizar los objetivos con el fin de establecer de forma clara lo que se busca con el trabajo de auditoría.

Podemos definir a un objetivo como el punto que pretenden alcanzar determinados individuos y/o grupos, por lo tanto la definición anterior es aplicable para la auditoría de sistemas ya que cuando se determinan los objetivos de esta se pretende anticipar lo que se desea satisfacer con ella.

Muñoz Razo, Carlos[11] incluye los siguientes puntos para el concepto de objetivo.

- *Misión. Deber moral que se impone a la realización de la auditoría de sistemas.*
- *Visión. La forma como se ve la realización de la auditoría y lo que se espera de ella.*
- *Propósitos. Objetivo que se pretende alcanzar con la auditoría.*
- *Metas. Fines específicos de la auditoría.*
- *Fines. Son los últimos aspectos que se busca satisfacer con la auditoría.*
- *Plazos. Los términos en unidades de tiempo en que se satisface el fin que se pretende con la auditoría.*

Los objetivos se pueden clasificar de la siguiente manera. Véase Ilustración 7.

Ilustración 3. Clasificación de los objetivos.

[11] Muñoz Razo, Carlos, Auditoría en sistemas computacionales, editorial Pearson Education.

A continuación se definirán cada uno de los objetivos que muestra la clasificación anterior.

Objetivo general. Es el fin global que el auditor pretende alcanzar con el desarrollo de la auditoría de sistemas. En este se determinan todos los puntos que se requieren evaluar, es decir, el establecimiento del objetivo general dará la idea global de lo que se va a cubrir con dicha auditoría y de esta forma propicia la realización de la misma.

Objetivo particular. Son los fines individuales que el auditor pretende alcanzar con el desarrollo de la auditoría de sistemas, estos pueden ser de alguna área, sistema o función particular.

Objetivos específicos. Son los fines que el auditor establece de forma concreta, pretendiendo desarrollar con ellos la auditoria de sistemas por lo que señala de forma específica las áreas, sistemas o funciones que evaluará.

Un ejemplo de objetivo para una auditoría de sistemas es:

- Evaluar los sistemas y procedimientos, así como la eficiencia de su uso y su relación con las necesidades de la organización.

2.2.4 Determinar los puntos específicos que serán evaluados.

En esta etapa el auditor deberá establecer los puntos específicos que serán evaluados en la auditoría de sistemas, dichos puntos deberán efectuarse considerando aspectos muy concretos de los sistemas tales como:

- Las funciones del personal informático y usuarios de los sistemas.
- Los recursos materiales y técnicos del área de sistemas.
- El análisis, diseño y desarrollo de los sistemas.
- La operación de los sistemas.
- La seguridad e integridad de los sistemas.

- La protección a las bases de datos.
- La documentación de los sistemas.
- entre otros aspectos.

Definir y establecer los puntos específicos que se evaluarán es muy importante para el auditor ya que estos son el resultado de un análisis previo de las etapas de identificación del origen de la auditoría, de la visita preliminar al área de sistemas y del establecimiento de los objetivos de la auditoría.

El análisis previo es muy importante ya que sin este es muy difícil establecer los puntos específicos que se evaluarán en la auditoría de forma correcta, es decir el auditor deberá especificar los aspectos de los sistemas que se van a evaluar, para después establecer las herramientas y la forma en que realizará dicha evaluación.

Por lo tanto la realización de una planeación deficiente, limitada y sin bases reales trae como consecuencia una evaluación de los sistemas errónea, por lo que el auditor tendrá serios problemas en la aplicación de las herramientas de auditoría y de esta forma los resultados que se obtengan de dicha planeación serán de dudosa calidad.

Los puntos que serán evaluados deberán ser desarrollados de acuerdo a los diversos criterios que se establezcan entorno al desarrollo de la auditoría como pueden ser:

- La experiencia, conocimientos y habilidades profesionales del auditor.
- Las necesidades de evaluación y la forma de procesamiento de información de la organización.
- Los métodos, técnicas y procedimientos que se aplicarán en la auditoría, etc.

A continuación se mencionarán algunos puntos específicos con el fin de mostrar un criterio de selección de aquellos aspectos que pueden ser tomados en cuenta en la evaluación de una auditoría de sistemas de información.

Los puntos específicos son. Véase Ilustración 8.

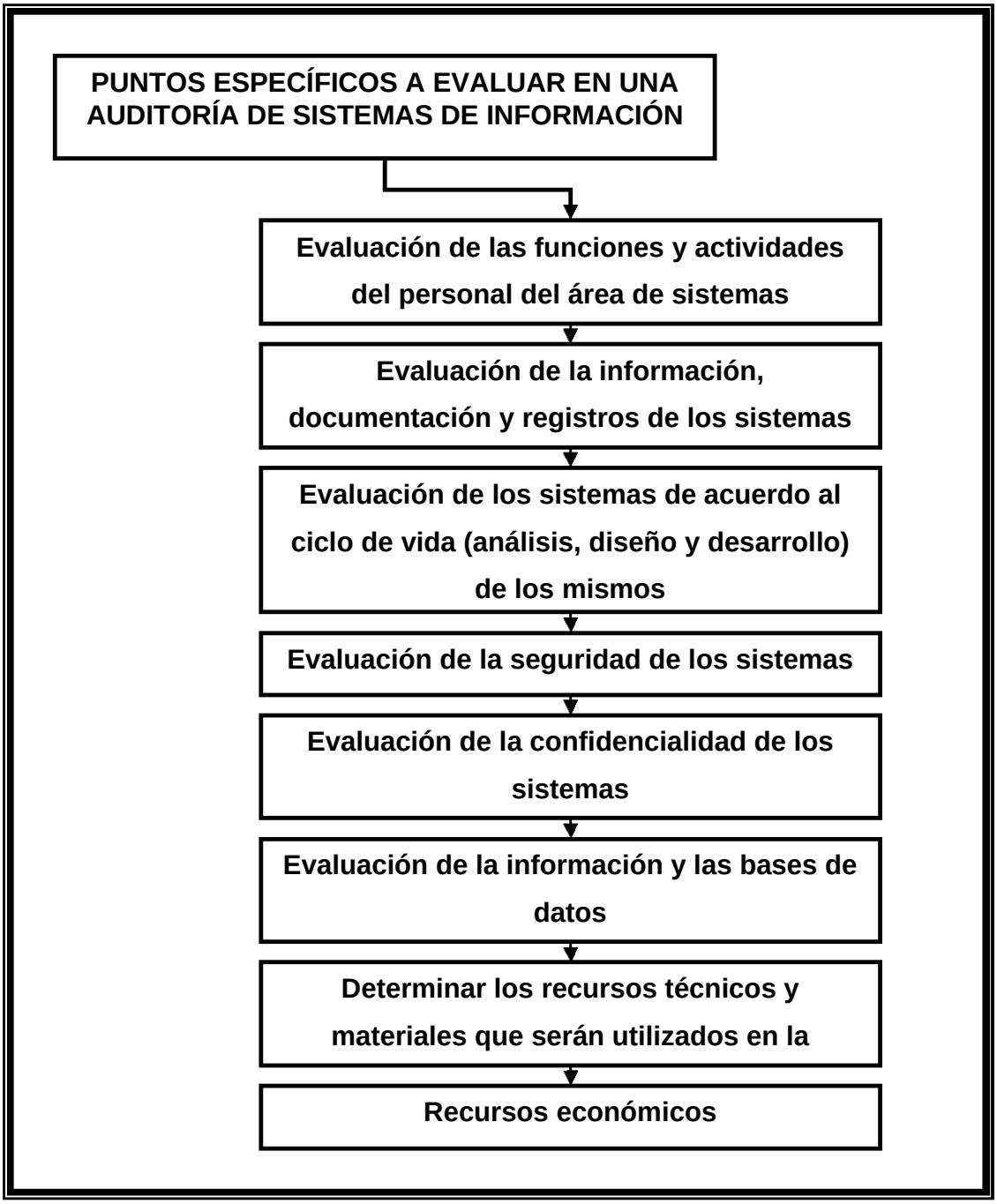

Ilustración 4. Puntos específicos a evaluar en una auditoría de sistemas de información.

2.2.5 Asignar los recursos que serán utilizados en la auditoría.

Después de haber identificado los puntos específicos que serán evaluados, se deberán establecer los recursos que se necesitarán para poder realizar la auditoría de sistemas de acuerdo con lo planeado y tomando en cuenta que dichos recursos son limitados.

En el caso especial de esta auditoría y por lo técnico del ambiente donde se realiza, los recursos que se le asignen deben ser muy especializados. A continuación se mencionarán los principales recursos que deberá tomar en cuenta el auditor para llevar acabo la auditoría. Véase Ilustración 9.

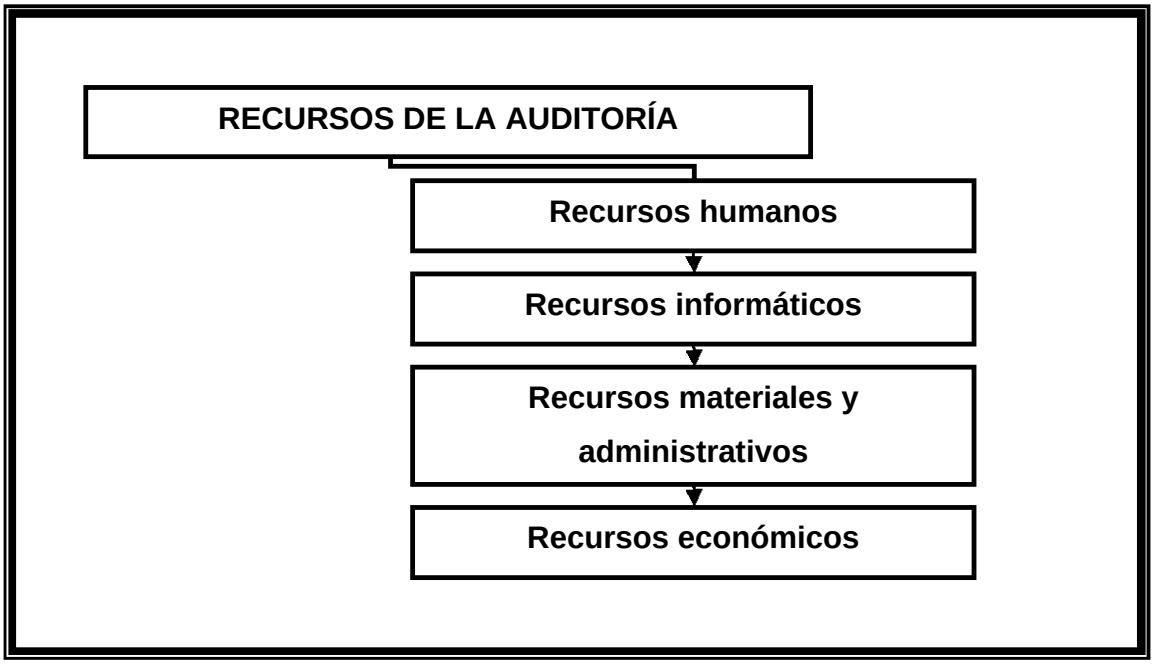

Ilustración 5. Recursos de la auditoría.

A continuación se detallarán los puntos mencionados en la ilustración anterior.

Recursos humanos. Una parte importante de la planeación de la auditoría es el personal especializado en informática y auditoría que deberá participar, ya que con ellos se realizan todas las actividades programadas para la revisión de los sistemas, la elaboración de pruebas, operación de los sistemas, la evaluación del funcionamiento de los sistemas, sus bases de datos, el uso correcto y adecuado de la información, y en sí de todos los aspectos que serán evaluados. Las principales características del personal que intervendrá en la auditoría de sistemas son:

- Personal altamente capacitado.
- Personal con alto sentido de moralidad.
- Personal eficiente.

- Personal con experiencia.
- El personal deberá recibir una retribución por su trabajo.

El personal de la auditoría de sistemas se clasifica de la siguiente forma:

- **Expertos en auditoría.** Este personal tiene que ser especializado en las técnicas y procedimientos de auditoría, pero también debe tener amplios conocimientos y experiencia en el área de sistemas por lo que es recomendable que los especialistas sean auditores en informática.

- **Personal del área de sistemas.** Es necesario que el auditor reciba apoyo de los expertos informáticos del área de sistemas para llevar acabo las pruebas, programas y procedimientos de evaluación de los sistemas a auditar, debido a que existen aspectos que solo el personal del área domina como pueden ser el tipo de sistemas, la plataforma que se utiliza etc. El personal del área de sistemas no está a disposición del auditor por lo tanto este no tiene ningún tipo de autoridad sobre el ni puede intervenir en su trabajo, el auditor solo puede pedir la cooperación de este para la realización de la misma. Entre los expertos informáticos encontramos, analistas, programadores, operadores, personal de bases de datos, entre otros.

Recursos informáticos. Después de haber asignado el personal que participará en la auditoría, se deberán asignar los recursos informáticos que requiere el auditor para realizar su evaluación, es decir, sus herramientas de trabajo. Estos recursos informáticos pueden ser:

- Hardware.
- Software de evaluación especializado para auditoría.
- Sistemas que utilizará durante su evaluación.
- Sistemas operativos.
- Programas de aplicación.
- Bases de datos e información del sistema, etc.

Recursos materiales y administrativos. La finalidad de asignar estos recursos es que el auditor lleve acabo su evaluación sin contratiempos al contar con el material necesario para desempeñar su trabajo. Estos recursos pueden ser oficinas privadas, mobiliario, equipo de oficina, papelería, así como el apoyo logístico, administrativo y secretarial necesario.

Recursos económicos. Otro punto importante para el desarrollo de una auditoría es el apoyo financiero que necesita el auditor para llevar acabo la misma, estos recursos se clasifican de la siguiente manera. Véase Tabla 4.

GASTO	DESCRIPCIÓN
Viáticos.	Es la cantidad de dinero que se le asigna al auditor ya sea por día, semana o cualquier otro periodo, con el fin de cubrir sus gastos de viaje, estancia y alimentación durante la evaluación de los sistemas de la organización.
Pasajes.	Es la cantidad de dinero que se entrega al auditor con el fin de cubrir su traslado al lugar donde llevara acabo su evaluación.
Otros gastos.	Es la cantidad de dinero que se entrega al auditor para cubrir sus gastos que se derivan de la realización de la auditoría, como pueden ser transporte, gasolina, casetas, derechos, compras de material informático, papelería o cualquier otro gasto.

Tabla 1. Clasificación de los recursos económicos.

El auditor deberá comprobar los gastos que efectué durante la evaluación o tal vez dichos gastos estarán exentos de ser comprobados, esto depende de las normas y políticas de la organización.

2.2.6 Elaborar los documentos necesarios para la auditoría.

Una vez que se han desarrollado cada una de las etapas anteriores, el siguiente paso es realizar la planeación formal de la auditoría de sistemas de información, es decir, se deben elaborar los documentos necesarios para la auditoría. La realización de la documentación formal se puede definir como la elaboración específica y cautelosa de los planes de trabajo para la auditoría de sistemas de información. Los documentos necesarios para la planeación de la auditoría de sistemas de información son:

- Programa de auditoría.
- Avance del cumplimiento del programa de auditoría.
- Carta convenio de servicios profesionales de auditoría de sistemas.
- Contrato de auditoría de sistemas.

A continuación se dará una breve explicación de cada uno de los documentos antes mencionados, además, se mostrarán los formatos propuestos para cada uno de ellos.

Programa de auditoría. Este documento resume el plan de trabajo de la auditoría, además, servirá de base para llevar un control adecuado del desarrollo de la misma. Véase Ilustración 10.

Avance del cumplimiento del programa de auditoría. Este documento permite el cumplimiento de los procedimientos de control y asegura que el trabajo se este realizando de acuerdo con el programa de auditoría. Véase Ilustración 11.

Carta convenio de servicios profesionales de auditoría en informática. Este documento manifiesta el compromiso que el auditor dirige a su cliente para que este le confirme su aceptación. Véase Ilustración 12.

Contrato de auditoría en informática. Este documento da a conocer el acuerdo de voluntades entre las partes (cliente-auditor) para llevar acabo la auditoría de sistemas. Véase Ilustración 13.

HOJA: ___ DE ___

AUDITORÍA EN SISTEMAS A.C.

EMPRESA: _____. FECHA DE FORMULACIÓN: _____.

AUDITOR: _____. ÁREA AUDITADA: _____.

PROGRAMA DE AUDITORÍA

FASE	DESCRIPCIÓN	ACTIVIDAD	RESPONSABLE	PERÍODO ESTIMADO		RECURSOS ESTIMADOS
				INICIO	TERMINO	

Ilustración 6. Ejemplo formato programa de auditoría de sistemas.

FECHA: _____

HOJA: ___ DE___

AUDITORÍA EN SISTEMAS A.C.

EMPRESA: _____. **PERÍODO: _____.**

AUDITOR: _____. **ÁREA AUDITADA: _____.**

AVANCE DEL CUMPLIMIENTO DEL PROGRAMA DE AUDITORÍA

FASE	SITUACIÓN DE LA AUDITORÍA			PERÍODO REAL	DÍAS REALES	GRADO DE AVANCE	EXPLICACIÓN DE LAS VARIACIONES
	NO INICIA	EN PROCESO	TERMINO	DEL _ AL_			

Ilustración 7. Ejemplo formato avance del cumplimiento del programa de auditoría de sistemas.

Ciudad de México, __ de_____de____.

AUDITORÍA EN SISTEMAS A.C.

NOMBRE DEL CLIENTE.
CARGO.
EMPRESA.

CARTA CONVENIO DE SERVICIOS PROFESIONALES DE AUDITORÍA EN INFORMÁTICA

Con un saludo me dirijo a usted, de la manera más atenta con el fin de presentarle la ***Propuesta de servicios profesionales para la realización de la auditoría de sistemas***, la cual se llevará acabo bajo los siguientes lineamientos.

PERIODO: Del__de____al__de____de_____.
HORARIO: De __:__ hrs. a __:__ hrs.

I. ANTECEDENTES.

[Anotar los antecedentes específicos del proyecto de auditoría de sistemas.]

II. OBJETIVOS DE LA AUDITORÍA.

[Anotar el objetivo específico de la auditoría de sistemas.]

III. ALCANCES DEL PROYECTO.

[Anotar los puntos específicos de evaluación que se desean alcanzar con la auditoría de sistemas.]

IV. METODOLOGÍA.

[Anotar los métodos de investigación que se utilizarán en el proyecto de auditoría.]

V. TIEMPO Y COSTO.

[Poner el tiempo en que se realizará el proyecto, de preferencia indicando el tiempo de cada una de las etapas; el costo del mismo, que incluya el personal participante en la auditoría y sus características, y la forma de pago.]

Sin otro particular, le agradezco su atención esperando una pronta respuesta.

ATENTAMENTE

FIRMA DEL AUDITOR

NOMBRE Y CARGO DEL AUDITOR

Ilustración 8. Ejemplo carta convenio de servicios profesionales de auditoría de sistemas.

Ciudad de México, __ de_____de____.

AUDITORÍA EN SISTEMAS A.C.

CONTRATO DE AUDITORÍA EN INFORMÁTICA

Contrato de prestación de servicios profesionales de auditoría en informática que celebran por una parte el **CLIENTE** _____ representado por _____ en su carácter de _____ y por otra parte _____ _____ representada por _____ _____ a quien se denominará el **AUDITOR**, de conformidad con las declaraciones y cláusulas siguientes:

DECLARACIONES

I. El cliente declara:

a. Que es una _____.
b. Que está representado para este acto por _____ _____ y que tiene como su domicilio _____ _____.
c. Que requiere obtener servicios de auditoría en informática, por lo que ha decidido contratar los servicios del auditor.

II. El auditor declara:

a. Que es una sociedad anónima, constituida y existente de acuerdo con las leyes y que dentro de sus objetivos primordiales está el de presentar auditoría en informática _____ _____.

b. Que está constituida legalmente según escritura número _____ de fecha _____ ante el notario público núm._____ 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 cláusulas siguientes:

CLÁUSULAS

Primera. Objeto. El auditor se obliga a prestar al cliente los servicios de auditoría en informática para llevar acabo la evaluación de la dirección de sistemas del cliente, que se detallan en la propuesta de servicios anexa que, firmada por las partes, forma parte integrante del contrato.

Segunda. Alcance de trabajo. [Anotar el alcance de los trabajos que llevará acabo el auditor dentro de este contrato.]

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 precisión las actividades a realizar por cada una de las partes, los responsables de llevarlas acabo y las fechas de realización.

Cuarta. Supervisión. El cliente tendrá 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. Coordinación de los trabajos. El cliente designará a un coordinador de proyecto, quien será responsable de recopilar la información que solicite el auditor, además se encargará de que las reuniones y entrevistas programadas se lleven acabo en las fechas establecidas.

Sexta. Horario de trabajo. El personal del auditor dedicará el tiempo necesario para cumplir satisfactoriamente con las actividades señaladas en el programa de trabajo convenido por ambas partes, además gozará de libertad fuera del tiempo destinado al cumplimiento de dichas actividades, por lo que no estará sujeto a horarios y jornadas determinadas.

Séptima. Personal asignado. El auditor designará para el desarrollo de los trabajos a socios del despacho, quienes, cuando consideren necesario, incorporarán personal técnico capacitado de que dispone la firma, en el número que se requieran y de acuerdo a los trabajos a realizar.

Octava. Relación laboral. El personal del auditor no tendrá ninguna relación laboral con el cliente y queda estipulado en este contrato que el auditor en ningún momento se considera intermediario del cliente respecto al personal que ocupe para dar cumplimiento de las obligaciones que se deriven de las relaciones entre él 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 cláusula segunda de este contrato en _____ días hábiles después de la fecha en que se firme el contrato y sea cobrado el anticipo correspondiente.

Décima. Honorarios. El cliente pagará a auditor por los trabajos objeto del presente contrato, honorarios por la cantidad de _____ más el impuesto al valor agregado correspondiente.

a. _____% a la firma del contrato.
b. _____% a los _____ días hábiles después de iniciados los trabajos.
c. _____% a la terminación de los trabajos y presentación del informe final.

Undécima. Alcance de los honorarios. El importe señalado en la cláusula décima compensará al auditor por sueldos, honorarios, organización y dirección técnica propia de los servicios de auditoría, prestaciones sociales y laborales de su personal.

Duodécima. Incremento de honorarios. En caso de que se tenga un retraso por causa del cliente, este contrato se incrementará en forma proporcional al retraso y se señalara el incremento de común acuerdo.

Decimotercera. Trabajos adicionales. De ser necesaria alguna adición a los alcances o productos del presente contrato, las partes celebrarán por separado un convenio que formará parte integrante de este instrumento y en forma conjunta se acordará el nuevo costo.

Decimocuarta. Viáticos y pasajes. El importe de los viáticos 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, será por cuenta del cliente.

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

Decimosexta. Causas de rescisión. Serán causas de rescisión de este contrato la violación o incumplimiento de cualquiera de las cláusulas de este contrato.

Decimoséptima. Jurisdicción. Todo lo no previsto en este contrato se regirá por las disposiciones relativas, contenidas en el Código Civil del _____ y, en caso de controversia para su interpretación y cumplimiento, las partes se someten a la jurisdicción de los tribunales federales, renunciando al fuero que les pueda corresponder en razón 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 día _____.

EL CLIENTE **EL AUDITOR**

Ilustración 9. Ejemplo de contrato de auditoría en informática.

Los documentos que el auditor deberá diseñar para la recopilación de datos son:

Cuestionarios. Los cuestionarios son las formas de recopilación de información más utilizadas y de mayor utilidad por el auditor, y consisten en recopilar datos, mediante la aplicación de papel con preguntas impresas, en donde el encuestado responde de acuerdo con su criterio, a fin de que el auditor concentre, agrupe y tabule las respuestas para obtener, por medio del análisis e interpretación, información significativa para poder evaluar lo que se esta auditando. A continuación se mostrará el formato propuesto de cuestionario. Véase Ilustración 14.

FECHA: _____

HOJA: ___ DE___

AUDITORÍA EN SISTEMAS A.C.

EMPRESA: _____. REALIZADO: _____.

ÁREA: _____. REVISADO: _____.

CUESTIONARIO DE AUDITORÍA DE SISTEMAS

1. Desarrollo.

	SI	NO	N/A
1.1 ¿Existen procedimientos adecuados para el desarrollo de sistemas?			
1.2 ¿Los desarrollos están basados en un conjunto formal de requerimientos de los usuarios?			
1.3 ¿El proceso de desarrollo incluye la necesidad de aprobación por parte del usuario, antes de proseguir en puntos clave como:			
1.3.1 Estudio de factibilidad.			
1.3.2 Propuestas del diseño del sistema.			
1.3.3 Especificaciones de diseño.			
1.3.4 Modificaciones al sistema antes de su implantación.			

Conclusiones de la sección revisada _____.

Ilustración 10. Formato de cuestionario.

Entrevista. Es la recopilación de información que se obtiene en forma directa, cara a cara, a través de algún medio de captura de datos, en donde el auditor interroga, cuestiona, investiga y confirma sobre los aspectos que está auditando, siguiendo una serie de preguntas preconcebidas, las cuales va adaptando conforme recibe la información del entrevistado y de acuerdo con las circunstancias que se le presentan para obtener mayor información. La entrevista es de gran utilidad para saber cómo opera un sistema, pero debe manejarse adecuadamente, por lo tanto el auditor debe contar con amplia experiencia y conocimientos para utilizarla, además deberá apoyarse a la guía de entrevista, en donde se definen todos los puntos que tendrá que seguir para que este instrumento sea útil y valioso para su trabajo de auditor. Los puntos que debe contener la guía de entrevista son. Véase Ilustración 15.

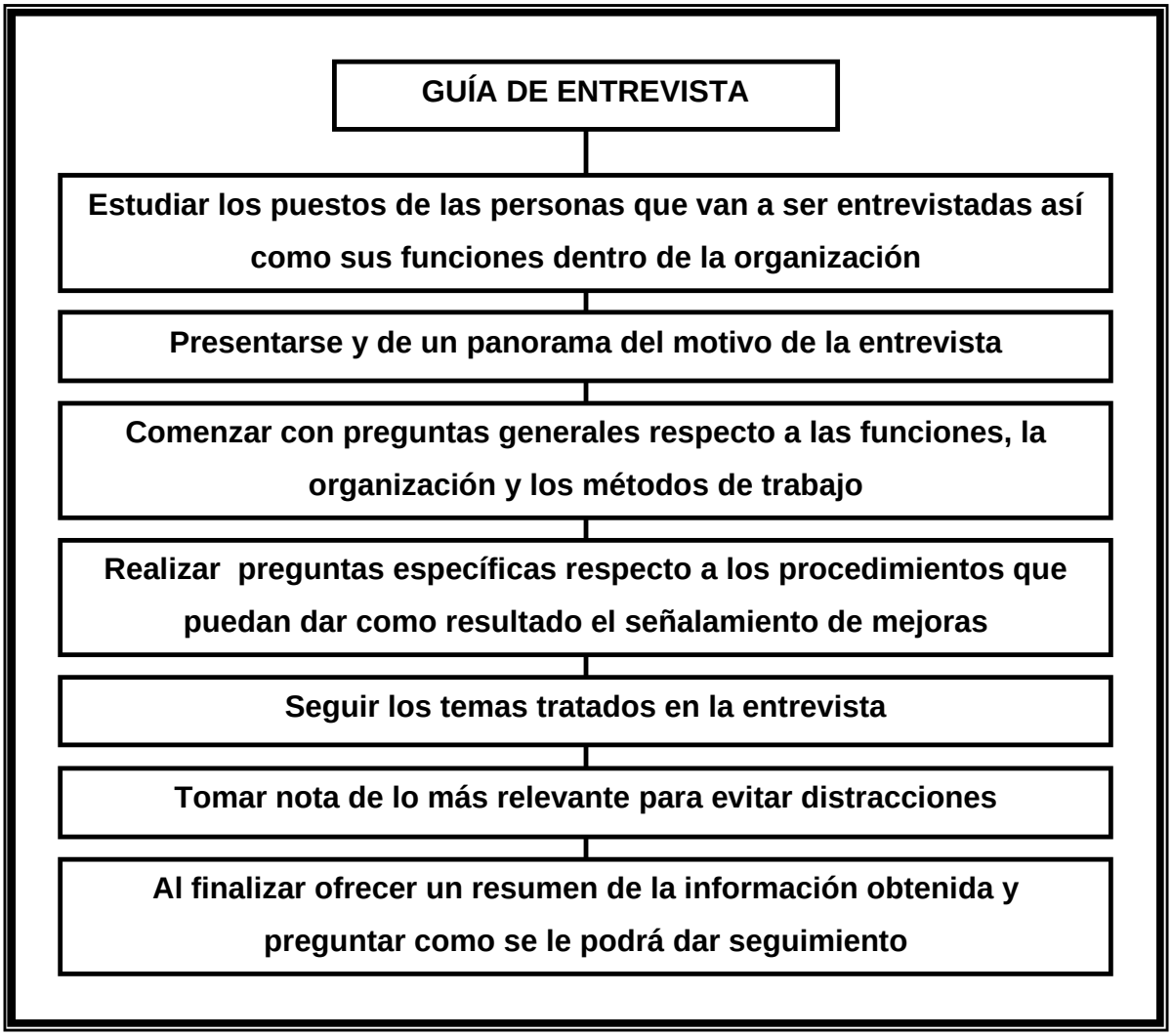

Ilustración 11. Guía de entrevista.

CAPÍTULO 3. EJECUCIÓN DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN.

3.1 Aplicar la auditoría de sistemas de información.

El siguiente paso después de la planeación de la auditoría es su ejecución, la cual deberá llevarse acabo de acuerdo con lo establecido en la etapa de planeación por lo tanto cada auditor deberá realizar las actividades que le corresponden de acuerdo como fueron diseñadas en el programa de auditoría, con el propósito de ejecutar los eventos programados y alcanzar el objetivo de la misma.

3.2 Metodología para la elaboración de sistemas de información.

Cada organización debe establecer una metodología para la elaboración de sus sistemas, es decir, deberá realizar su propio modelo del Ciclo de Vida del Desarrollo de Sistemas (CVDS), con el fin de controlar el proceso de desarrollo de los mismos. La siguiente tabla muestra los puntos que debe contener dicha metodología y los puntos que el auditor evaluará de esta. Véase Tabla 5.

CONTENIDO	PUNTOS A EVALUAR POR EL AUDITOR
Etapas del CVDS.	Evaluar si la división de etapas es coherente con la metodología que, por lo general, se aplica en los sistemas y si cada una de ellas da lugar a un producto final cuantificable.
Funciones y responsabilidades del CVDS.	El auditor deberá revisar la asignación de las funciones y responsabilidades de las diversas etapas de la metodología del CVDS, evaluando el grado de participación que tienen cada uno de los integrantes del proyecto en la toma de decisiones de cada una de las etapas del CVDS, además debe constatar que dichas funciones y responsabilidades existan y que se encuentren por escrito.
Actualización del CVDS.	Deberá evaluar si la metodología del CVDS utilizada por la organización continua siendo provechosa.

Tabla 1. Contenido y puntos a evaluar en la metodología de desarrollo de sistemas.

3.3 Evaluación de sistemas de información de acuerdo con el Ciclo de Vida del Desarrollo de Sistemas (CVDS).

Evaluación de sistemas de información. Podemos definir la evaluación de sistemas de información como el proceso mediante el cual el auditor responsable y su equipo se encargan de revisar todos los aspectos relacionados con los sistemas con el fin de optimizar el buen desempeño, confiabilidad y seguridad de los mismos.

Seen, James[12], define Ciclo de Vida del Desarrollo de Sistemas (CVDS) como:
Es el conjunto de actividades que los analistas, diseñadores y usuarios realizan para desarrollar e implantar un sistema de información.

Los sistemas deben ser evaluados de acuerdo con el CVDS que normalmente siguen, por lo tanto la presente tesis propone las diversas etapas del CVDS para la realización de la auditoría de sistemas de información. Véase Ilustración 16.

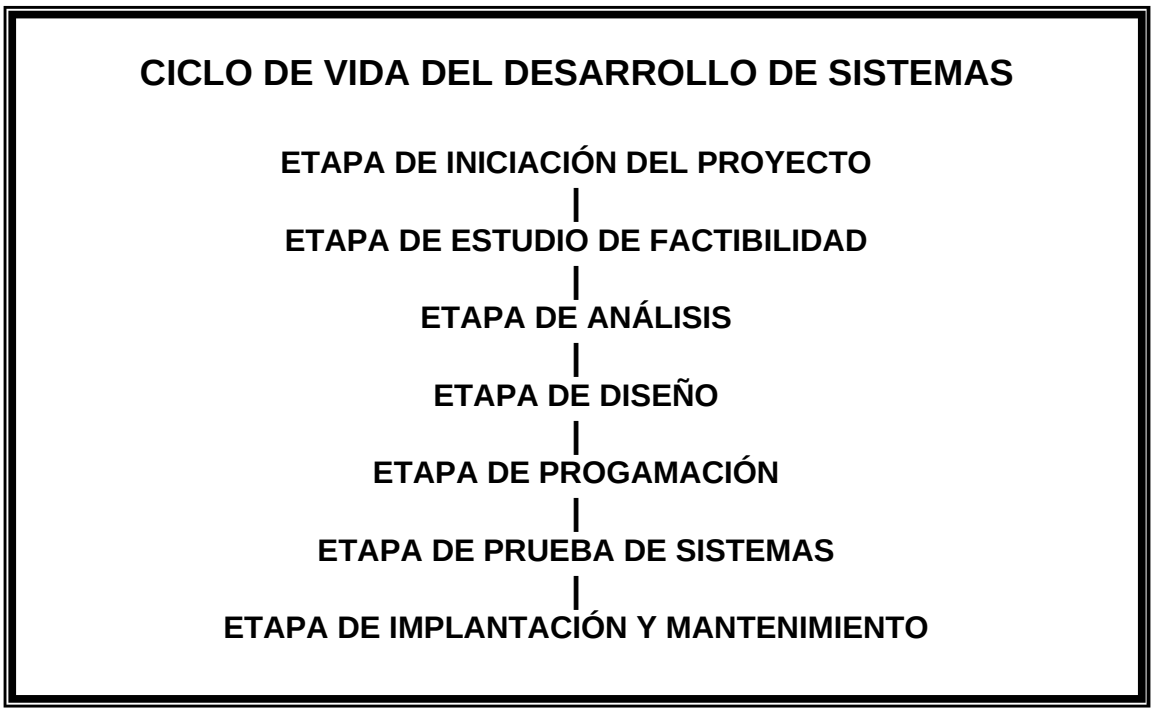

Ilustración 1. Etapas propuestas para el Ciclo de Vida del desarrollo de Sistemas.

[12] Seen, James, Análisis y diseño de Sistemas de Información, editorial Mc Graw Hill.

En los siguientes puntos se detallarán cada una de las etapas del Ciclo de Vida del Desarrollo de Sistemas que muestra la ilustración anterior, las cuales fueron propuestas para llevar acabo la auditoría de sistemas de información.

3.3.1. Etapa de iniciación del proyecto.

Evaluación de la participación de la dirección del departamento usuario. El primer aspecto que deberá evaluar el auditor en ésta etapa es la participación de la dirección del departamento usuario en la iniciación del proyecto, por lo tanto el auditor debe llevar acabo las siguientes acciones. Véase Tabla 6.

PARTICIPACIÓN DE LA DIRECCIÓN DEL DEPARTAMENTO USUARIO	
Acciones a realizar por el auditor.	— Analizar las minutas del comité de planeación para comprobar la participación de la dirección del departamento usuario. — Examinar la planeación del proyecto para conocer el origen y el alcance de la participación de la dirección del departamento usuario. — Entrevistar a la dirección del departamento usuario con el fin de conocer su grado de participación en el proyecto. — Revisar el presupuesto asignado por la dirección del departamento usuario para la realización de los sistemas de información.

Tabla 2. Acciones que llevará acabo el auditor para evaluar la participación de la gerencia del departamento usuario.

Así el ciclo de vida del desarrollo de sistemas (CVDS) comienza cuando algún departamento usuario de la organización realiza una solicitud de proyecto para la elaboración de un sistema de información que cubra sus necesidades para llevar acabo sus funciones. Dicha solicitud es enviada primeramente a la dirección del departamento usuario, el cual deberá analizarla para después rechazarla o aprobarla.

Evaluación de la solicitud del proyecto. Para llevar acabo ésta evaluación el auditor deberá pedir la solicitud del proyecto con el propósito de revisar los siguientes puntos. Véase Tabla 7.

SOLICITUD DEL PROYECTO	
Puntos a evaluar	— Confirmar que la solicitud se encuentre por escrito y que incluya los puntos establecidos como requisitos del proyecto (justificación, ambiente, alcance, restricciones y beneficios), además el auditor deberá cerciorarse de que el equipo del proyecto haya definido los requerimientos de información del proyecto en dicha solicitud. — Comprobar que la solicitud concuerde con el plan aprobado por el comité de planeación de sistemas de información para el presente año. — Verificar que la documentación del proyecto sea realizada con el modelo del CVDS de la organización.

Tabla 3. Puntos a evaluar de la solicitud del proyecto.

Evaluación de la aprobación de la solicitud del proyecto. El auditor deberá confirmar que la solicitud del proyecto haya sido revisada por la dirección del departamento usuario y que ésta haya dado por escrito su aprobación al departamento usuario para continuar con la siguiente etapa del CVDS.

Después de haber evaluado la etapa de iniciación del proyecto, el auditor deberá evaluar la siguiente etapa del CVDS que es el estudio de factibilidad.

3.3.2. Etapa de estudio de factibilidad.

Cuando el departamento de sistemas recibe una solicitud de proyecto de algún departamento usuario deberá realizar un estudio de factibilidad con el propósito de analizar si el sistema propuesto es susceptible de realizarse.

El estudio de factibilidad debe contener los siguientes puntos. Véase Ilustración 17.

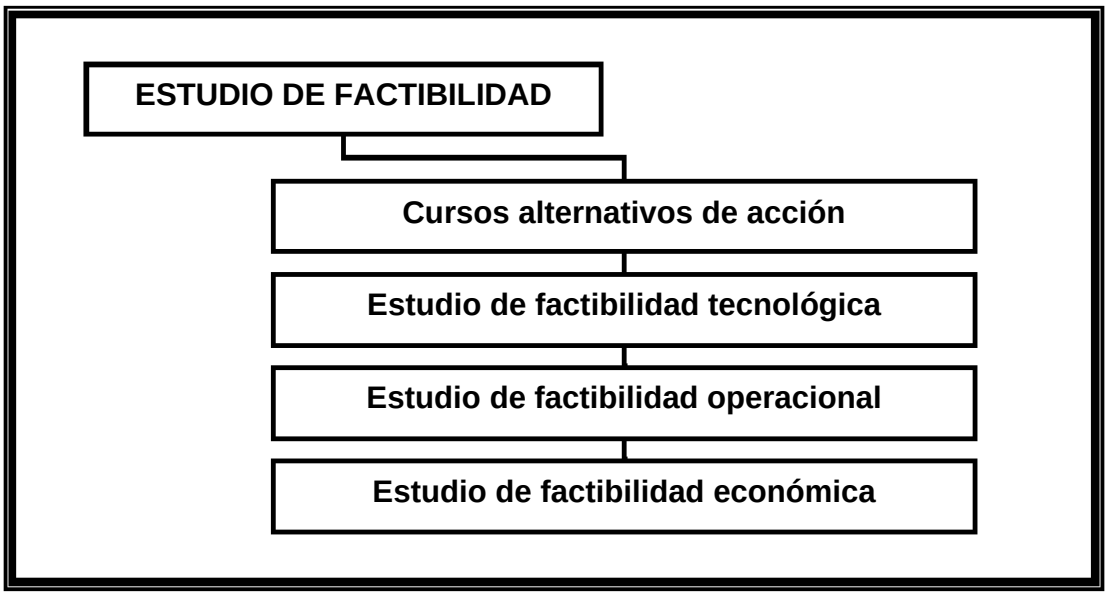

Ilustración 2. Contenido del estudio de factibilidad.

Para realizar la evaluación de ésta etapa el auditor deberá solicitar el estudio de factibilidad del sistema con el propósito de evaluar su contenido.

Cursos alternativos de acción. Son las diferentes alternativas que se preparan y analizan con el propósito de sustentar que la realización del sistema es viable, por lo tanto cada alternativa deberá satisfacer lo requerimientos de información del nuevo sistema.

Los puntos que evaluará el auditor son:

- Deberá analizar la descripción y documentación de todos los cursos alternativos de acción con el propósito de confirmar que estos satisfagan los requisitos de información del nuevo sistema.
- Asegurarse de que los cursos alternativos de acción sean factibles y que éstos se enfoquen en los puntos de discusión del informe aprobado por la gerencia del departamento usuario.
- Confirmar que se sustente de forma adecuada el curso de acción recomendado y que éste sea el más factible.

Estudio de factibilidad tecnológica. El estudio de factibilidad tecnológica busca asegurar que la tecnología seleccionada funcionará de manera correcta y sin deteriorar el sistema, una vez puesto en operación y por la vida del mismo, es decir, que la aplicación soportará cambios sustanciales en la tecnología sin tener que realizar modificaciones importantes en él.

Los puntos que evaluará el auditor son:

1. Se debe preparar un estudio de factibilidad tecnológica para cada alternativa. Por lo tanto el auditor deberá revisar los informes de los estudios de factibilidad tecnológica para ver si se han enfocado adecuadamente los siguientes puntos:

   — Necesidades de equipo y su disponibilidad.
   — Necesidades de software del sistema y su disponibilidad.
   — Equipo de comunicaciones y su disponibilidad.
   — Restricciones de espacio y tiempo.

2. Examinará el informe del estudio de factibilidad tecnológica para comprobar si se tomaron en cuenta los siguientes aspectos legales relativos a la tecnología:

   — Consideraciones legales respecto a la transferencia nacional o internacional de tecnología o información.
   — Restricciones legales relativas al uso de tecnología y trámites para obtener la aprobación de la autoridad correspondiente.

3. Confirmar que exista un acuerdo entre el departamento usuario y los diseñadores, acerca de los aspectos tecnológicos del proyecto.

Estudio de factibilidad operacional. El auditor deberá revisar el estudio de factibilidad operacional con el propósito de asegurarse de que el sistema una vez puesto en operación funcionará de acuerdo con los criterios bajo los cuales se diseñó y que no ofrecerá problemas de carácter técnico ni administrativo.

Estudio de factibilidad económica. Se debe preparar un análisis de los costos y beneficios del proyecto con el propósito de evaluar la factibilidad económica de cada alternativa.

Los puntos que evaluará el auditor son:

- Revisar el resumen de los costos estimados para cada alternativa y los beneficios que reportará el sistema.
- Verificar que los costos del usuario y de los sistemas de información cubran todas las fases del CVDS.
- Confirmar que en los costos estimados de una alternativa se incluyan el equipo y las mejoras de software.
- Comprobar que los costos estimados de una alternativa incluyan los costos de entrenamiento, preparación, entrada de datos, conversión de archivos, pruebas, operaciones en paralelo, aceptación y costos relativos, en el lugar donde se apliquen.
- Verificar que los servicios estén cuantificados, hasta donde sea posible.
- Verificar que exista un acuerdo firme entre los usuarios finales, diseñadores, el personal de desarrollo y el de implantación acerca de los costos del sistema, los beneficios y los requisitos contractuales.

Aprobación del estudio de factibilidad. La dirección de informática debe revisar los informes de los diversos estudios de factibilidad y tomar la decisión de continuar o de no hacerlo, si decide continuar ésta deberá elegir una de las alternativas como punto de partida para las etapas siguientes.

Cuando la desición es continuar entonces el auditor deberá revisar la decisión de la dirección de informática, indicada por escrito y la alternativa seleccionada, además deberá evaluar los siguientes puntos:

- Revisar que los informes del estudio de factibilidad hayan sido preparados y turnados a la dirección de informática para su revisión.

— Confirmar que los informes del estudio de factibilidad hayan sido revisados por la dirección de informática y verificar si ésta tomó la decisión de continuar, con base en estos informes.
— Revisar la documentación que apoya la decisión de continuar además de la documentación de la alternativa seleccionada para un estudio posterior.

Plan maestro del proyecto. El siguiente paso después de la aprobación del estudio de factibilidad es la elaboración del plan maestro del proyecto.

Por lo tanto el auditor deberá revisar que éste incluya los procedimientos adecuados para mantener el control sobre el proyecto de desarrollo además deberá confirmar que éste contenga un método para controlar los costos durante las diversas fases del CVDS.

3.3.3. Etapa de análisis.

Cuando la dirección de informática aprueba el proyecto y entrega al departamento de sistemas la alternativa elegida entonces éste deberá comenzar a trabajar en el análisis del sistema. En esta etapa el auditor deberá evaluar los siguientes puntos. Véase Ilustración 18.

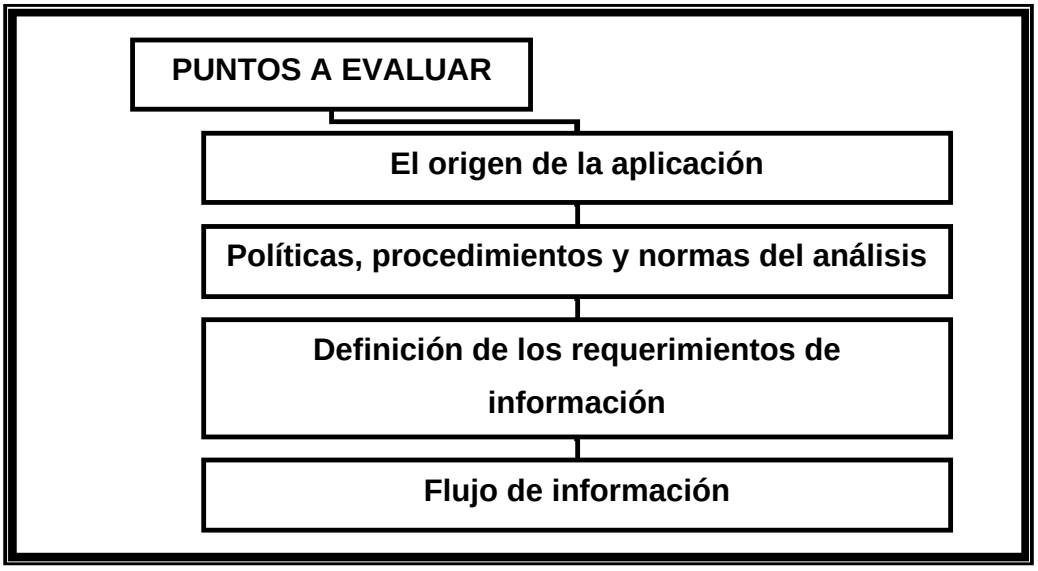

Ilustración 3. Puntos a evaluar en la etapa de análisis.

El origen de la aplicación. El auditor debe evaluar como surge la necesidad de desarrollar un nuevo sistema de información, éste se puede originar por cuatro fuentes principales:

- Planeación estratégica.
- Requerimientos de la organización.
- Requerimientos de los usuarios.
- El inventario de sistemas.

Además deberá revisar que el origen de la aplicación se encuentre documentada de forma detallada.

Las políticas, procedimientos y normas del análisis. El auditor deberá evaluar la forma en que se encuentran especificados las políticas, los procedimientos y las normas del análisis, además deberá revisar que se cumplan y que sean las adecuadas para la organización.

Definición de los requerimientos de información. El análisis debe incluir una definición de los requerimientos de información, por lo tanto el auditor debe confirmar que los analistas comprendan la información que necesitan los usuarios para realizar su trabajo.

El auditor deberá evaluar los siguientes puntos:

- Revisar las herramientas que utilizó el analista para definir los requerimientos de información del sistema (entrevistas, investigación de los datos relevantes, muestreo, cuestionarios, etc.).
- Deberá revisar la definición de los requerimientos de información.
- Vigilar que se evalúen los requerimientos de información para garantizar su integridad, consistencia y factibilidad de procesamiento.
- Verificar que la documentación relacionada con los requerimientos de informaciones prepare de acuerdo con los estándares del CVDS.

- Confirmar que los requisitos de información han sido revisados y aprobados por la dirección del departamento usuario, de tal forma que se cubran las necesidades de éste de acuerdo con las políticas de la organización.

Flujo de información. El flujo de información se puede definir como la secuencia lógica de las acciones del sistema.

El diagrama lógico del flujo de datos es la herramienta que se utiliza para elaborar el modelo gráfico del sistema mediante el uso de símbolos, este es muy útil porque detecta los procesos lógicos, los requerimientos de información, el flujo de información, y brinda un modelo gráfico del sistema.

No olvidemos que el diagrama lógico de flujo de datos del sistema propuesto se convierte en la base para desarrollar y evaluar las diferentes alternativas de diseño. Por lo tanto el auditor deberá solicitar los diagramas lógicos de flujo del sistema con el propósito de evaluar los siguientes puntos.

- ¿Es fácil de usar?
- ¿La secuencia es lógica?
- ¿Se encontraron errores?
- ¿Existen faltas de control?
- Analizar la ruta de 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 como llega a su destino.
- Revisar los diagramas de flujo del sistema para asegurarse de que cumple con las necesidades del usuario.
- Revisar los diagramas de flujo del sistema para observar el seguimiento del diseño general, si se observan cambios, el auditor deberá verificar que estos han sido discutidos y aprobados por los usuarios afectados.

La siguiente ilustración muestra un ejemplo de un diagrama de flujo de datos de un sistema de procesamiento de pedidos. Véase Ilustración 19.

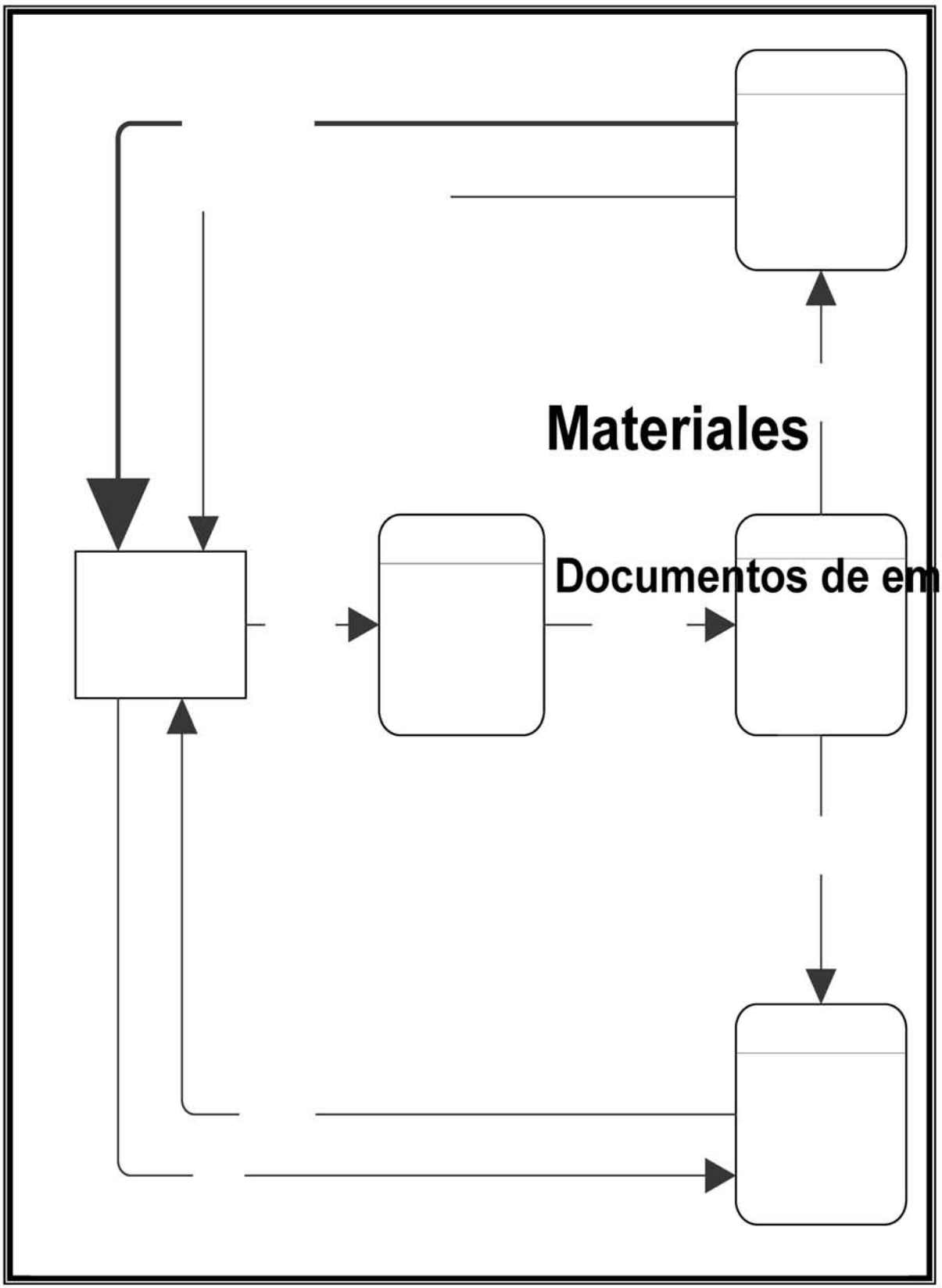

Ilustración 4. Diagrama de flujo de datos de un sistema de procesamiento de pedidos.[13]

[13] Grudnitski, Burch, Diseño de sistemas de información, Teoría y practica, Editorial LIMUSA.

Cliente Pedido

Pro

Después de haber evaluado la etapa de análisis, el auditor deberá evaluar la siguiente etapa del CVDS que es el diseño del sistema.

3.3.4. Etapa de diseño.

En esta etapa se debe diseñar el sistema de información que cumpla con todos los requerimientos del usuario, encontrados en la etapa de análisis, de tal forma que se diseñe el sistema correcto. Por lo tanto el auditor deberá evaluar los siguientes puntos. Véase ilustración 20.

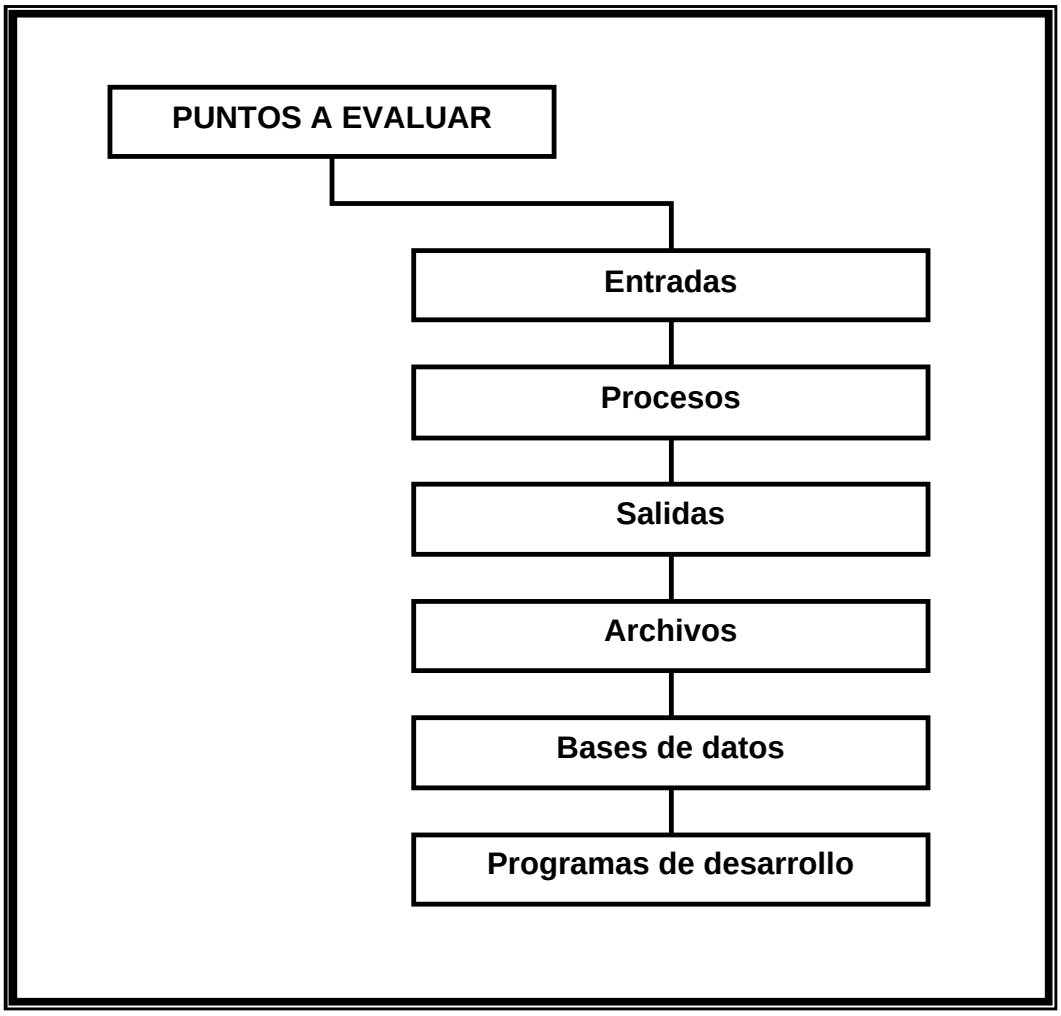

Ilustración 5. Puntos que deberá evaluar el auditor en la etapa de diseño.

Entradas. Es el proceso mediante el cual el sistema de información toma los datos que requiere para procesar la información. Los puntos que deberá evaluar el auditor son:

Definición de los requerimientos de entrada. Deben definirse y documentarse todos los requisitos de entrada. El auditor deberá revisar la definición y documentación relacionada con los requisitos de entrada.

1. Revisar que la documentación sobre los requisitos de entrada del sistema sea exacta y que contenga los siguientes puntos:

   — Requisitos de edición y validación.
   — Revisiones de seguridad para proteger su exclusividad.
   — Establecimiento de controles adecuados.
   — Autorización de entradas y actualización.

2. Confirmar que la dirección del departamento usuario haya revisado y aprobado, por escrito, las definiciones de entrada.

Diseño de documentos fuente. Deben diseñarse detalladamente los documentos fuente para entrada de la información, para facilitar la obtención y la entrada exacta de la información. El auditor deberá revisar la documentación relacionada con el diseño de los documentos fuente.

— Examinar las formas de los documentos de entrada para determinar si su diseño responde a las necesidades del departamento usuario.
— Revisar las formas de los documentos de entrada para determinar si contienen todas las condiciones para controles, como prefoliados y autorizaciones de transacción.
— Analizar las formas de los documentos de entrada para determinar si su diseño facilita la obtención de la información y promueve la exactitud mediante dispositivos tales como espacios exactos o alguna notación.
— Cuando la entrada de datos se registra por medio de sistema en línea, revisar el formato de la pantalla para determinar si éste facilita la obtención de la información, si utiliza comandos o instrucciones para registrarlos en forma adecuada o exacta y si tiene rutinas de edición para reducir los errores.

A continuación se mostrará el formato propuesto para la evaluación de formas. Véase Ilustración 21.

HOJA: ___ DE ___

AUDITORÍA EN SISTEMAS A.C.

Nombre de la forma.	**Frecuencia de uso.**	
Elaborado por.	**Num. de forma**	**Num. de copias**
Usuarios.	**Cantidad. impresa**	**Cantidad. inv.**
	Periodo estimado de uso.	

PUNTOS A EVALUAR

Información de la empresa.		**Imagen.**	
Terminología estándar.	SI NO	Profesional y correcta.	SI NO
Existe manual de operación.	SI NO	Calidad apropiada de papel.	SI NO
Autodescriptiva.	SI NO	Buena calidad de impresión.	
Fuente de información identificada	SI NO	**Costo.**	
Requiere otros datos de referencia.	SI NO	Máximo aprovechamiento de	
Tiene suficientes espacios.	SI NO	papel.	SI NO
Datos que contiene.		Máximo aprovechamiento de	
Necesita datos adicionales.	SI NO	impresión.	SI NO
Tiene datos innecesarios.	SI NO	Cumple con las necesidades.	SI NO
		Duplica datos de otras formas.	SI NO

Si la respuesta ha sido “NO” a alguna pregunta, anote las observaciones.

_____

_____

_____

Ilustración 6. Ejemplo de formato de evaluación de formas.

Procesos. Son los pasos que definen el uso específico de cada uno de los elementos del sistema. El auditor deberá evaluar las siguientes especificaciones:

- ¿Qué deberá hacer el sistema?
- ¿Cómo lo deberá hacer?
- ¿Cuál es la justificación para que se haga de la manera señalada?
- ¿Quién hace la función, cuándo y cómo?

El auditor deberá revisar el análisis relacionado con la definición y la documentación de las especificaciones para el procesamiento.

- Revisar las especificaciones de procesamiento para determinar si son adecuadas y si fueron preparadas de acuerdo con las políticas de la organización.
- Confirmar que la dirección del departamento usuario ha revisado y aprobado por escrito las especificaciones del procesamiento.

Además el auditor deberá revisar lo siguiente:

- Confirmar la capacidad del sistema de información para efectuar los cálculos.
- Verificar que los cálculos se realicen mediante una secuencia de operaciones preestablecidas.
- Revisar si los cálculos se efectúan con datos recién ingresados al sistema o con datos que ya están almacenados.

Salidas. Es la capacidad que tiene el sistema para sacar la información procesada o bien datos de entrada al exterior. Los puntos que deberá evaluar el auditor son:

Definición de los requisitos de salida. Se deberán definir y documentar todos los requisitos de salida del sistema. Por lo tanto el auditor deberá revisar la definición y documentación relacionada con los requisitos de salida y verificar que contenga los siguientes puntos:

— Contenido y formato de los informes preparados.
— Autorización de los usuarios para recibir los informes.
— Periodos de retención de los informes.
— Periodo de retención de los archivos.

Diseño de informes. Deben diseñarse detalladamente los informes para la salida de la información. El auditor deberá revisar los informes de salida para determinar si su diseño responde a las necesidades del departamento usuario. A continuación se mostrará el formato propuesto para la evaluación de informes. Véase Ilustración 22.

FUNCIÓN: _____

AUDITORÍA EN SISTEMAS A.C.

Nombre del informe.	
Propósito del informe.	
Quién lo formula.	
Qué lo origina.	
Volumen de hojas o registros.	
Forma de hacerlo.	
Principal usuario.	
Fecha teórica de presentación.	**Periodicidad.**
Fecha de presentación.	**Periodicidad.**
Nivel de información.	
En vigor desde.	
Modificaciones.	
Otros datos.	

TANTOS	**COLOR**	

DATOS QUE CONTIENE	ORDEN DE LOS DATOS

Ilustración 7. Ejemplo de formato de evaluación de informes.

Archivos. Deben definirse y documentarse todos los archivos y los métodos de organización de éstos. Los puntos que evaluará el auditor son:

- Revisar el análisis de la selección de los métodos de organización de archivos, con la definición y formatos de archivos.
- Determinar si se han proporcionado definiciones para todos los archivos, así como los métodos de organización adecuados.
- Determinar si el administrador de la base de datos ha participado en la definición y documentación de los requisitos de archivo y los métodos de organización de los mismos.
- Verificar si en el proceso de definición del archivo se han tomado en cuenta los niveles de seguridad, en relación con la sensibilidad de los datos.
- Examinar la documentación de las necesidades y los tipos de archivos con el fin de determinar si fueron revisados y aprobados por la dirección del departamento usuario.

Bases de datos. Echenique García, José Antonio[14] define a una base de datos como:

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.

[14] Echenique García, José Antonio, Auditoría en informática, editorial Mc Graw Hill.

En las bases de datos se deben evaluar los siguientes puntos:

- La independencia de los datos.
- Redundancia de los datos y archivos.
- Consistencia de los datos.
- Almacenamiento de los datos.
- Revisar que los datos se encuentren organizados en archivos de forma uniforme y consistente.
- Revisar que el acceso a la información sea uniforme y consistente.

Los componentes a evaluar dentro de una base de datos son:

- Diccionario.
- Lenguajes de datos: DDL (Lenguajes de Descripción de Datos, DML (Lenguajes de Manipulación de Datos).
- Software de seguridad.
- Herramientas de desarrollo de aplicaciones.
- Sistemas de almacenamiento, respaldo y recuperación.
- SQL (Structured Query Language).
- Directorio de datos.

Programas de desarrollo. Es el software que se usará para codificar la aplicación. Los puntos que evaluará el auditor son:

Especificaciones de la aplicación. Las especificaciones de programas deben prepararse por escrito y de forma detallada, para permitir que los programadores codifiquen la aplicación.

- Revisar que las especificaciones para cada aplicación del sistema sean claras, completas y consistentes.
- Revisar los diagramas de flujo para validar la lógica de la programación incorporada en las aplicaciones.

Software. Al utilizar un determinado software se debe evaluar lo siguiente:

- Interfases de usuario gráfico con el fin de poder diseñar pantallas agradables y visuales.
- Enlace de objetos.
- Capacidad de trabajar en multiplataformas.
- Capacidad de trabajar en redes.
- Licencias.
- Transportable.
- Compatible con otro software.
- Fácil de usar.
- Nivel de sofisticación.
- Capacidad de utilización en red.
- Fácil instalación.
- Demanda de hardware.
- Requerimientos de memoria.
- Costo.
- Seguridad y confidencialidad.

Después de haber evaluado la etapa de diseño, el auditor deberá evaluar la siguiente etapa del CVDS que es programación.

3.3.5 Etapa de programación.

Cuando los diseñadores entregan a los programadores las especificaciones del software completas y claramente definidas, éstos deben iniciar la codificación de la aplicación.

Programación. Se define como una serie de instrucciones que se le indican a la computadora para realizar una determinada tarea, dichas instrucciones se realizan por medio de un software. Los puntos que deberá evaluar el auditor son. Véase Ilustración 23.

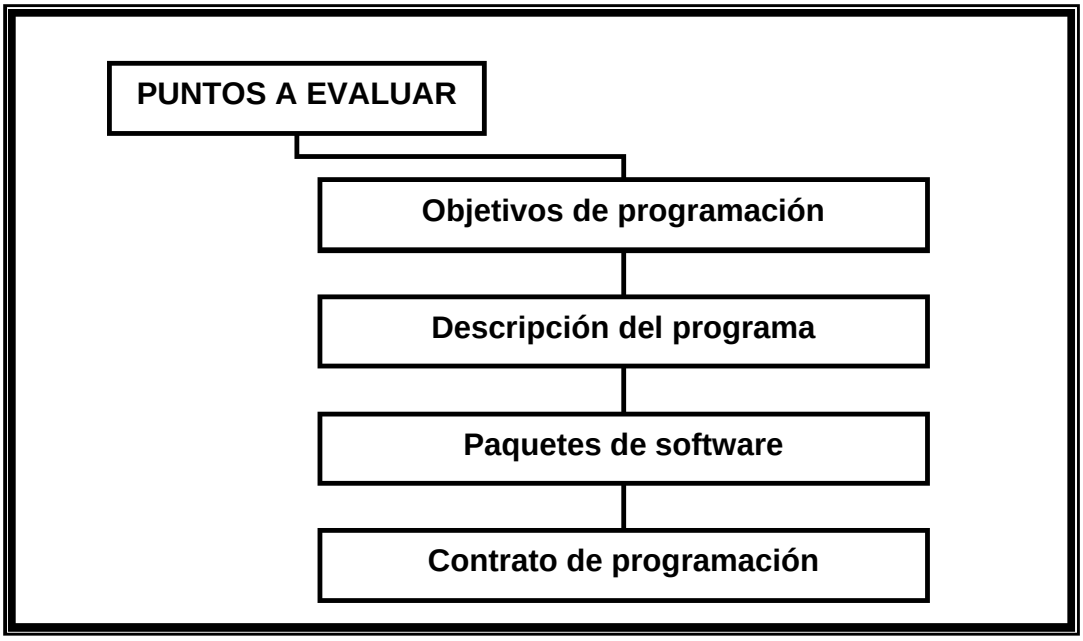

Ilustración 8. Puntos a evaluar en la etapa de programación.

Objetivos de programación. Cada proyecto que requiera programación, debe contar con un informe de los objetivos del programa, el cual debe contener la descripción del propósito, las funciones que deberán realizarse, la entrada utilizada, la salida producida y los archivos generados.

Por lo tanto el auditor deberá solicitar el informe de los objetivos de programación con el propósito de evaluar los siguientes puntos:

- Revisar los postulados de los objetivos para asegurarse de que describen adecuadamente los programas y sus funciones.
- Confirmar si estos postulados de objetivos se apegan a los estándares de documentación de programas vigentes en la organización.

Descripción del programa. Cada programa debe incluir una descripción o instructivo detallado del procesamiento y de su lógica. El auditor deberá evaluar lo siguiente:

- Revisar los instructivos detallados que se prepararon como parte de la documentación del programa, para determinar su extensión y verificar si están de acuerdo con la definición original del sistema.

- Revisar la descripción detallada de la lógica, para confirmar si está escrita de forma clara y concisa, de manera que las personas que no conozcan bien el programa puedan entender su función.
- Comprobar si los estándares de documentación requieren un diagrama de flujo a nivel programa y si la documentación existente cumple con este requisito.
- Verificar si se ha desarrollado un diagrama de flujo a nivel de programas y confirmar que esté actualizado y se apegue a la definición del programa.
- Obtener descripciones de archivos para programas seleccionados y confirmar si éstas describen con precisión los archivos, los registros y los campos para los datos, incluyendo las definiciones de los códigos y registros.
- Confirmar que las descripciones de los archivos se adecuan a los estándares de documentación de la organización.

Paquetes de software. Se debe hacer un análisis para determinar la disponibilidad de software comercial de paquete, que pueda satisfacer las necesidades de la organización y que sea compatible con las operaciones del sistema de información para realizar la programación.

La adquisición de paquetes de software debe seguir todas las políticas de adquisición de la organización y éstos deben probarse y revisarse antes de utilizarlos y pagarlos.

Los puntos que evaluará el auditor son:

- Revisar las políticas y los procedimientos de compra de paquetes de software aplicativo.
- Examinar los informes del estudio económico de factibilidad, para determinar si se tomaron en cuenta para este estudio las consideraciones acerca de la compra de los paquetes.
- Analizar los acuerdos para la adquisición de paquetes de software, para determinar si las condiciones del contrato son congruentes con las políticas de adquisición de la organización.

- Confirmar que los acuerdos de adquisición contengan una aprobación, por escrito, de la dirección del departamento de sistemas de información y del departamento usuario.
- Revisar la documentación referente a la adquisición para determinar si el paquete de software fe aprobado y revisado antes de usarlo y pagarlo.
- Examinar los paquetes de software y toda su documentación para determinar que éstos, así como los controles incorporados y su documentación sean adecuados.

Contrato de programación. Se debe realizar un contrato para la programación mediante una solicitud de servicio suscrita por el gerente del proyecto. Los proyectos terminados deben probarlos y revisarlos, los miembros del grupo directivo de sistemas de información, antes de autorizar su pago. Los puntos que evaluará el auditor son:

- Revisar los procedimientos de solicitud de contrato para programación de aplicaciones y para prueba.
- Analizar los requisitos del contrato de servicios de programación para determinar si son razonables y si intervino en su aprobación el departamento de sistemas de información.
- Examinar el contrato de servicios para determinar si los servicios esperados están establecidos claramente y que contengan todas las condiciones para casos de contingencia e incumplimiento.
- Confirmar que las partes que están proporcionando los servicios de programación conocen los estándares de documentación de programas de la organización, así como los objetivos y los instructivos de los programas.
- Evaluar la documentación para determinar si el grupo de control de calidad o el de sistema de información ha revisado y aprobado los códigos, la documentación y los controles en los programas desarrollados bajo contrato, y si estos programas se apegan a los estándares de documentación de programas de la organización.
- Interpretar la documentación para determinar si los programas desarrollados bajo contrato se probaron con base en los estándares de prueba de la organización.

— Revisar la documentación respecto a las erogaciones de la empresa con el fin de determinar si los pagos por servicios de programación se amparan en documentación y si éstos han sido aprobados.

Características de los sistemas. Las características que deben evaluarse en los sistemas son:

— Dinámicos (susceptibles de modificarse).
— 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).
— Jerárquicos (por niveles funcionales).
— Seguros (que sólo las personas autorizadas tengan acceso).
— Únicos (que no duplique información).

Después de haber evaluado la etapa de programación, el auditor deberá revisar los siguientes manuales. Véase Ilustración 24.

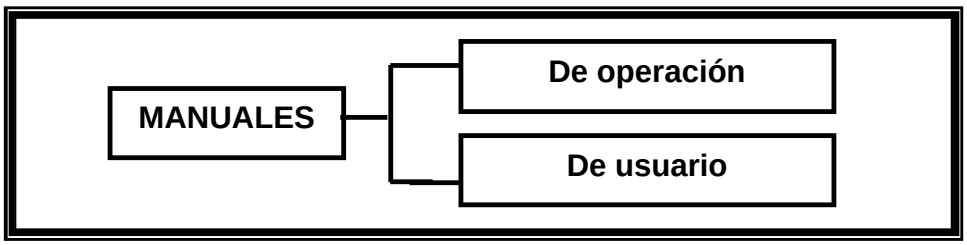

Ilustración 9. Manuales que evaluará el auditor.

Manual de operación. Se debe preparar y documentar de forma adecuada los manuales de operación. Los puntos que deberá evaluar el auditor respecto a los manuales de operación son:

1. Confirmar que los estándares de documentación de programas, definen la documentación necesaria para cada aplicación.
2. Revisar que existan manuales de operación individuales y que se apeguen a los estándares de documentación de programas de la organización.
3. Asegurarse de que cada manual de operación contenga la información necesaria de cada programa de la cadena de trabajo para el operador.
4. Verificar que para cada operación, la documentación especifique:

   - Función del programa.
   - Requisitos de hardware.
   - Diagrama de flujo por cada programa.
   - Diagrama particular de entrada/salida.
   - Mensaje y su explicación.
   - Parámetros y su explicación.
   - Diseño de reimpresión de resultados.
   - Cifras de control.
   - Fórmulas de verificación.
   - Instrucciones en caso de error.
   - Calendario de proceso y resultados.
   - Observaciones.

5. Confirmar que los manuales de operación se usen en los procesos de prueba.
6. Confirmar que los manuales de operación estén al alcance de los operadores y que éstos los lean y comprendan punto por punto.

Manual de usuario. Se debe preparar y documentar de forma adecuada los manuales de usuario. Los puntos que deberá evaluar el auditor respecto a los manuales de usuario son:

1. Confirmar que haya manuales de usuario y que se defina toda la documentación que necesita el usuario en cada aplicación.
2. Verificar que los estándares de documentación de programas definan la documentación necesaria para el usuario en cada aplicación.
3. Asegurarse de que en cada manual del usuario exista información adecuada para que se puedan preparar los datos de entrada que serán procesados, que se entienda la asignación de prioridades, el tiempo probable de respuesta y la recepción del producto de sistemas de información.
4. Confirmar que cada manual de usuario, contenga la siguiente documentación:

   - Especificaciones y diseños de entrada de datos.
   - Necesidades de control.
   - Formas de presentar los datos al departamento de sistemas de información.
   - Responsabilidad de la conversión de datos al lenguaje de máquina.
   - Responsabilidad para resolver errores o algún otro problema.
   - Asignación de prioridades para el proceso.
   - Calendario y frecuencia de la distribución de las salidas.
   - Seguridad, vigencia y disposición de salidas.
   - Lógica de programación.
   - Deducción de fórmulas importantes.
   - Registro de aprobación del usuario.
   - Registro de aprobación de la solicitud de cambios en el programa.
   - Procedimiento para encender y apagar terminales.
   - Descripción de las pantallas y de los comandos disponibles.

5. Confirmar que los manuales de usuario se usen en los procedimientos de prueba.
6. Asegurarse de que los manuales de usuario se distribuyan de acuerdo con las políticas de la organización.

Después de haber evaluado los manuales de operación y de usuario, el auditor deberá evaluar los controles para la realización de los sistemas.

3.3.5.1 Control de proyectos.

Es muy común que la implantación de los sistemas se retrase porque éstos no han sido terminados, debido a que no existe una planeación para controlar el avance de los sistemas, por lo tanto se recomienda que se utilice la técnica de administración por proyectos para su adecuado control.

Cuando un sistema es liberado en el plazo establecido y dentro del presupuesto, significa que el grado de control en el desarrollo del mismo es el adecuado o tal vez el óptimo. Para poder controlar el avance de los sistemas, ya que ésta es una actividad de difícil evaluación, se recomienda que se utilice la técnica de administración por proyectos para su adecuado control.

Para 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.

Dicho plan debe ser revisado de forma periódica ya sea semanalmente, mensualmente, etc., para evaluar el avance respecto a lo programado. La estructura estándar de la planeación de proyectos deberá incluir:

- Control de proyectos.
- Calendario de actividades (Gráfica de Gantt).
- Control de actividades del programador.
- Reporte semanal de los responsables de sistemas.
- Control de programadores.
- Planeación de programación.
- Hoja de planeación de actividades.
- Informe de avance de programación.
- Control de avance de programación.
- Hoja de planeación de actividades.
- Control de avance.

La evaluación de proyectos y su control puede realizarse con el siguiente cuestionario:

1. ¿Existe una lista de proyectos de sistema de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro?
2. ¿Está relacionado el plan maestro con un plan general de desarrollo de la dependencia?
3. ¿Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios?
4. ¿Asigna el plan maestro un porcentaje del tiempo total de producción al reproceso o fallas de equipo?
5. Escribir la lista de proyectos a corto plazo y largo plazo.
6. Escribir una lista de sistemas en proceso periodicidad y usuarios.
7. ¿Quién autoriza los proyectos?
8. ¿Cómo se asignan los recursos?
9. ¿Cómo se estiman los tiempos de duración?
10. ¿Quién interviene en la planeación de los proyectos?
11. ¿Cómo se calcula el presupuesto del proyecto?
12. ¿Qué técnicas se usan en el control de los proyectos?
13. ¿Quién asigna las prioridades?
14. ¿Cómo se asignan las prioridades?
15. ¿Cómo se controla el avance del proyecto?
16. ¿Con qué periodicidad se revisa el reporte de avance del proyecto?
17. ¿Cómo se estima el rendimiento del personal?
18. ¿Con que frecuencia se estiman los costos del proyecto para compararlo con lo presupuestado?
19. ¿Qué acciones correctivas se toman en caso de desviaciones?
20. ¿Qué pasos y técnicas siguen en la planeación y control de los proyectos? Enumérelos secuencialmente.

    1. ( ) Determinación de los objetivos.
    2. ( ) Señalamiento de las políticas.
    3. ( ) Designación del funcionario responsable del proyecto.
    4. ( ) Integración del grupo de trabajo.

5. ( ) Integración de un comité de decisiones.
6. ( ) Desarrollo de la investigación.
7. ( ) Documentación de la investigación.
8. ( ) Factibilidad de los sistemas.
9. ( ) Análisis y valuación de propuestas.
10. ( ) Selección de equipos.

21. ¿Se llevan a cabo revisiones periódicas de los sistemas para determinar si aún cumplen con los objetivos para los cuales fueron diseñados?

De análisis	SÍ ( )	NO ( )
De programación	SÍ ( )	NO ( )

Observaciones.

A continuación se mostrará un ejemplo de control de proyectos, usando la Gráfica de Gantt. Véase Ilustración 25.

Ilustración 10. Ejemplo de Gráfica de Gantt.

Después de haber evaluado el control de proyectos, el auditor deberá evaluar las pruebas del sistema.

3.3.6 Etapa de prueba de sistemas.

Prueba de sistemas. En ésta etapa, el sistema se utiliza de manera experimental para asegurar que el software no tenga fallas, es decir, busca comprobar que la aplicación cumpla con las especificaciones del usuario, que se haya desarrollado dentro de los presupuestado, que tenga los controles necesarios y que efectivamente cumpla con los objetivos y beneficios esperados.

Las pruebas del sistema tratan de garantizar que se cumplan los requisitos de las especificaciones funcionales, verificando datos estadísticos, transacciones, reportes y archivos, anotando las fallas que pudieran ocurrir y realizando los ajustes necesarios, así los niveles de prueba peden agruparse en módulos, programas y sistema total. Los puntos que se toman en cuenta para la prueba de un sistema son:

- Prueba particular de cada programa.
- Prueba por fase, validación, actualización.
- Prueba de corrida en paralelo.
- Prueba de seguridad y confidencialidad.
- Prueba de calidad entre otras.

El departamento de sistemas de información debe preparar para cada sistema que se ha desarrollado o que ha sido sujeto a una revisión importante, la documentación referente a las pruebas del sistema. Por lo tanto el auditor debe solicitar dicha documentación con el propósito de evaluar los siguientes puntos:

- Confirmar que la solicitud para la realización de pruebas se encuentra por escrito y aprobada por la dirección del departamento de sistemas de información y por la dirección del departamento usuario.
- Analizar la asignación de responsabilidades de prueba de sistemas, con la finalidad de conocer qué personal es responsable de la preparación de los datos de la prueba y de la aprobación y confirmar si el personal ha aceptado dichas responsabilidades.

- Elegir sistemas representativos que hayan sido desarrollados o sujetos a modificaciones importantes durante el año anterior y determinar si se preparó un plan de prueba para ellos.
- Revisar los resultados de las pruebas de los sistemas elegidos y determinar si éstas contienen todos los elementos importantes y si la dirección y el personal de departamento usuario revisaron y aprobaron de forma simultánea los resultados.
- Discutir procedimientos y resultados de la prueba con el departamento usuario.
- Evaluar si el personal del departamento usuario está consiente de la importancia de las pruebas, de su grado de participación y si se consideran responsables de la aprobación de los resultados de estas pruebas.
- Revisar la información de la prueba (listados de datos de la prueba, los reportes o salidas del sistema de información etc.) para verificar que los resultados esperados se desarrollaron de forma anticipada, se compararon con los resultados de la prueba y que ambos concordaron.
- Cuando los resultados de las pruebas no sean los esperados, revisar las diferencias y buscar las causas.
- Si es necesario, analizar los resultados con la dirección del departamento usuario o con la del departamento de sistemas de información.
- Revisar los resúmenes escritos de las evaluaciones de los resultados de las pruebas y determinar si dichas evaluaciones se realizaron y si, en caso de existir, los problemas se resolvieron antes de poner en operación el nuevo sistema.
- Confirmar que la dirección del departamento usuario ha revisado el funcionamiento del nuevo sistema, si considera que es adecuado y satisface sus necesidades.
- Determinar si la dirección del departamento usuario ha reconocido cualquier falla en el nuevo sistema y si ésta ha sido corregida y se tiene la aprobación de la dirección del departamento usuario.
- Analizar la aceptación final del sistema por parte de la dirección del departamento usuario y del departamento de sistemas de información.

Después de haber evaluado la etapa de prueba de sistemas, el auditor deberá evaluar la siguiente etapa del CVDS que es implantación y mantenimiento.

3.3.7 Etapa de implantación y mantenimiento.

Implantación. Esta etapa se inicia solo después de una exitosa etapa de prueba. La implantación consiste en instalar el nuevo sistema de información en la empresa, así como impartir la capacitación necesaria a los usuarios para que éstos aprovechen todas las ventajas que ofrece el nuevo sistema.

El auditor debe confirmar que la implantación del sistema de información se encuentre por escrito y aprobada por la dirección del departamento de sistemas de información y por la dirección del departamento usuario, además debe revisar la documentación del sistema a fin de asegurarse de que está completo y que todas las actualizaciones posteriores a la fase de prueba han sido incorporadas.

Los puntos que debe evaluar el auditor en esta etapa son:

1. Plan de trabajo para la implantación del nuevo sistema.
2. Cronograma de actividades.
3. Hardware que se utilizará en la instalación del nuevo sistema.
4. Programación final del sistema de información, es decir, verificar la construcción de todos los archivos de datos necesarios para correr la aplicación con la finalidad de asegurare de que es correcta y que esta completa.
5. Verificar la instalación de las bases de datos con la finalidad de asegurare de que es correcta, además deberá evaluar la forma en que se van a cargar los datos en el sistema.
6. Capacitación del usuario. Confirmar que los usuarios fueron capacitados antes de instalar la nueva tecnología y analizar el tipo de capacitación que recibieron.

Cuando el sistema se ha implantado, lo primero que deberá hacer el auditor es asegurarse de que el sistema sea operacional, es decir, que funcione de acuerdo a los requerimientos del análisis, por lo tanto deberá permitir a los usuarios operarlo. El auditor deberá revisar los siguientes puntos respecto a los procedimientos de control de operación del nuevo sistema.

- Revisar la descripción de los procedimientos de control del departamento usuario y del de sistemas de información, para determinar si están completos y si son adecuados para el tipo de archivos que se mantienen y para las transacciones que procesa el nuevo sistema.
- Resolver si los procedimientos de control incluyen controles adecuados de distribución de salidas, de manera que sólo las reciba el personal autorizado del departamento usuario.
- Comprobar si la dirección del departamento usuario revisó y aprobó los procedimientos de control.

Mantenimiento. Una vez instalados, los sistemas de información, éstos se usarán durante muchos años. Sin embargo, las organizaciones y los usuarios cambian con el paso del tiempo, incluso el ambiente es diferente con el paso de las semanas y los meses. Por lo tanto, es indudable que debe darse mantenimiento a los sistemas de información.

Los puntos que debe evaluar el auditor respecto a las modificaciones del sistema son:

- Confirmar que las modificaciones del sistema se encuentren por escrito y aprobadas por la dirección del departamento de sistemas de información y por la dirección del departamento usuario.
- Analizar la efectividad de los procedimientos de modificación del sistema.
- Investigar y asegurar que existe un registro cronológico de todos los cambios.
- Revisar el proceso de evaluación de los cambios o modificaciones propuestos para el sistema que está en operación.
- Investigar si se registran los requisitos de cambio o modificación, en caso de que así sea, evaluar la oportunidad del procesamiento de dichos requisitos.
- Cuando se ha modificado un sistema en operación, revisar su documentación para saber si esas modificaciones forman parte integral de ella.
- Investigar si dicha documentación incluye los requisitos de las modificaciones, la aprobación de tales requisitos, las descripciones de las modificaciones que se

han realizado, la actualización de los diagramas de flujo o tablas de decisión, los resultados de prueba y la aprobación del departamento usuario.

Después de haber evaluado todas las etapas del ciclo de vida del desarrollo de sistemas (CVDS), el auditor deberá realizar una evaluación final.

3.4 Evaluación final.

Después de que se ha implantado un sistema de información, debe hacerse una evaluación final con el propósito de determinar si éste ha logrado los objetivos iniciales del proyecto de desarrollo.

Por lo tanto evaluará los siguientes puntos:

Cumplimiento de los requisitos de usuario.

1. Determinar si el personal de sistemas de información o de control de calidad realiza rutinariamente evaluaciones para medir el grado de satisfacción del usuario, para determinar si se cumplieron sus requisitos y necesidades.
2. Revisar los reportes preparados por el personal de sistemas de información o de control de calidad, referentes a la satisfacción de los requerimientos del usuario con el nuevo sistema y determinar si el alcance de estos reportes cubre lo siguiente:

   — Revisión de la definición original de los requisitos del usuario en comparación con el uso del sistema existente.
   — Determinación del grado en que cumple el sistema con las necesidades de la dirección del departamento usuario.
   — Análisis del nivel de satisfacción de acuerdo con la información proporcionada por el nuevo sistema.
   — Relación de las modificaciones sugeridas para el sistema, con el fin de identificar el desempeño existente del sistema y el esperado.

Resultados del procesamiento.

1. Determinar si el personal de sistemas de información o de control de calidad evalúa rutinariamente los resultados de proceso, para determinar si se han cumplido los objetivos originales.
2. Revisar los reportes preparados por el personal de sistemas de información o de control de calidad y determinar si abarcan los siguientes puntos:

   — ¿La operación del nuevo sistema está de acuerdo con los objetivos y las especificaciones originales?
   — Si se encontraron errores ¿se investigaron y solucionaron adecuadamente?
   — Si hubo ineficiencias ¿se reportaron éstas y sus soluciones se evaluaron adecuadamente?

Análisis de costo beneficio. Comparar los beneficios y costos estimados originalmente con los costos y beneficios obtenidos. La siguiente ilustración muestra un ejemplo de análisis de costos y beneficios de un sistema para la recepción de pedidos y cuentas por cobrar. Véase ilustración 26.

COSTOS INICIALES DEL SISTEMA.

Desarrollo.	
Análisis de sistemas y determinación de requerimientos.	
Semanas (160 horas)	6,000
Diseño de sistemas.	
Semanas (240 horas).	9,000
Desarrollo e implantación.	
Semanas (480 horas).	18,000
Costos indirectos generados por el personal.	2,500
Compra de equipo.	
IBM AS/400	40,000
Tres terminales a 600 dólares cada una.	1,800
Mobiliario.	2,500
Instalación.	
Preparación del local.	1,000
Entrenamiento.	3,750
Generación del sistema.	750
Costos totales para el inicio.	**$85,300**

COSTOS DE OPERACIÓN DEL SISTEMA.

Suministros.
Mantenimiento adicional del equipo.
Programa de mantenimiento.

Costos totales de operación (primer año). **$10,000**

BENEFICIOS DEL SISTEMA.

Ahorros por no necesitar más personal.	22,100
Ahorros de operación.	
Eliminación de errores en los precios (mínimo)	5,000
Disminución del saldo de las cuentas por cobrar.	20,000

Beneficios intangibles.
Mejor información para planificación.
Mejores relaciones con los clientes.
Empleados más satisfechos con su trabajo.
Necesidad de crecer.
Posibilidad de aumentar la comunicación y evitar costos asociados con el correo (si se da la expansión).

Total de beneficios tangibles del sistema (primer año). **$47,100**

TIEMPO DE VIDA DE CINCO AÑOS

Año	Costos del Sistema	Beneficios del sistema	Diferencia neta acumulativa
1	$85,300	$47,100	$38,200
2	11,000	24,300	10,900
3	12,500	26,750	50,150
4	15,000	29,400	89,550
5	17,000	32,300	**$129,850**
	$140,800	**$159,850**	

La recuperación de la inversión ocurre entre 17 y 18 meses después del inicio del proyecto.

Ilustración 11. Análisis de costos y beneficios.[15]

[15] Seen, James, Análisis y diseño de Sistemas de Información, editorial Mc Graw Hill.

CAPÍTULO 4. DICTAMEN DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN.

4.1 El informe de auditoría.

Informe de auditoría. El informe es el documento más importante de la auditoría de sistemas de información, debido a que a través de éste se presentan los resultados obtenidos durante la evaluación, en él se reportan, por escrito, las observaciones y el dictamen que emite el auditor.

4.2 Procedimiento para elaborar el informe de auditoría.

El auditor debe seguir una serie de pasos ordenados para elaborar el informe de auditoría. Los pasos para realizar dicho informe son:

1. **Aplicar los instrumentos de recopilación.** El auditor debe aplicar los instrumentos, técnicas, procedimientos y herramientas que diseño en la etapa de planeación, con el propósito de detectar las posibles desviaciones en la operación normal del sistema de información que está auditando, de acuerdo con sus conocimientos y experiencia realiza un análisis comparativo de la operación normal contra la esperada. Una vez hecho este análisis, entonces puede definir aquellas situaciones que considera como desviaciones y las reporta como situaciones encontradas.

2. **Registrar las desviaciones halladas durante la revisión en el formato de situaciones encontradas.** Las desviaciones que reporta el auditor se deben plasmar por escrito en un documento de carácter formal, al que llamaremos *formato de situaciones encontradas*[16], cabe aclarar que dependiendo de la experiencia y habilidad del auditor, éste puede optar por elaborar un borrador de las situaciones encontradas, esto es con el propósito de que el auditor comente primeramente las desviaciones encontradas con los auditados, y después de comentarlas realice las modificaciones pertinentes, así como el informe definitivo de las situaciones encontradas.

[16] En el punto 4.4 se mostrará el formato de situaciones encontradas.

3. **Comentar las desviaciones encontradas con los auditados.** Una vez que el auditor ha detectado las desviaciones es su obligación discutirlas en forma directa y abierta con los auditados, ya que de alguna forma, éstos son los responsables de que se presenten dichas situaciones, el propósito de informarles es que conozcan, acepten, aclaren, complementen y/o las modifiquen con detalles y pruebas. Esto le sirve al auditor para complementar la redacción de las situaciones que reporta. Además comentar las desviaciones con el personal auditado le permite al auditor preparar las posibles soluciones así como las posibles causas.

4. **El auditor deberá encontrar las causas y posibles soluciones de las desviaciones encontradas junto con los auditados.** Al conocer las desviaciones que se le imputan, el auditado tratará de defenderse, señalando las causas que originaron cada una de las desviaciones encontradas, por lo tanto el auditor puede obtener de manera directa y en voz de los involucrados, las posibles soluciones a estas desviaciones. Incluso hasta los responsables de llevarlas acabo y la fecha compromiso para solucionar cada una de las desviaciones presentadas. Es importante que el auditor consiga la firma de enterado del auditado que deberá solucionar las desviaciones, pero si el auditado se negara a proporcionar su firma, no le afectaría al auditor para realizar su reporte, ya que dicha firma no influye en el resultado de la auditoría.

5. **Analizar, depurar y corregir las desviaciones encontradas.** Una vez que se comentaron las desviaciones con los auditados, y se obtuvieron las causas y posibles soluciones, entonces cada auditor debe entregar al responsable de la auditoría de sistemas de información el informe de situaciones encontradas, con el propósito de que éste analice las desviaciones, a fin de redactarlas mejor, concentrarlas y darles una estructura jerárquica.

6. **Jerarquizar las desviaciones encontradas y concentrar las más importantes en el formato de situaciones relevantes.** Después de haber supervisado que el informe de situaciones encontradas esté correctamente elaborado, el responsable de la auditoría de sistemas de información debe analizar las

desviaciones reportadas, a fin de escoger las que considere más importantes para reportarlas en el *formato de situaciones relevantes*[17], el propósito es remarcar lo que se considera como lo más importante de la evaluación practicada, a fin de que los directivos conozcan los aspectos más relevantes. Las situaciones que se reportan como las más relevantes se deben redactar tal y como fueron reportadas en el formato de situaciones encontradas, sin modificarlas, esto es para evitar confusiones de interpretación y errores mecanográficos o cualquier otra alteración de lo que se desea reportar como relevante.

7. **Comentar las situaciones relevantes con los directivos del área de sistemas y confirmar las causas y soluciones.** Así como las situaciones encontradas se comentaron con los auditados, también las situaciones relevantes se deben comentar con los directivos del área de sistemas, a fin de que éstos las conozcan. El personal auditado puede, a juicio de los directivos, estar presente para cualquier posible aclaración sobre lo informado, esto es lo más recomendable. El responsable de la auditoría debe encabezar la presentación de este informe al directivo de mayor jerarquía del área de sistemas. Por lo general, esta reunión es de carácter formal y en ella se reportan todas y cada una de las situaciones consideradas como relevantes, aunque también se pueden presentar las llamadas situaciones encontradas. Además, si el encargado de la auditoría lo considera pertinente, cada auditor puede presentar el informe de la parte que le tocó evaluar, o puede hacerlo una sola persona en representación del responsable de la evaluación. Todo se hace de acuerdo con el estilo y costumbre de realizar estas presentaciones. Como resultado de esta reunión, se pueden elaborar las modificaciones que a caso requiera y, de ser necesario, se puede convocar a una nueva reunión para presentar las situaciones relevantes.

8. **Concentrar, depurar y elaborar el informe final de auditoría, así como el dictamen del auditor.** El auditor responsable de la auditoría de sistemas de información debe depurar cada una de las situaciones relevantes reportadas, con el fin de concentrarlas en el informe final de auditoría. Debido a que el informe es

[17] En el punto 4.4 se mostrará el formato de situaciones relevantes.

para el área directiva de la empresa debe ser breve y solo deberá señalar lo más relevante de la evaluación, incluyendo el dictamen del auditor (opinión del auditor). Generalmente los directivos de la empresa son ajenos a la informática, por lo tanto, el informe final debe ser lo más sencillo, claro y comprensible para ellos. La elaboración del informe es el verdadero trabajo del responsable de la auditoría, debido a que en este documento es donde realmente se muestra la importancia de su actividad.

9. **Presentar el informe y dictamen final a los directivos de la empresa.** El último paso del informe de auditoría de sistemas de información es la presentación oficial del dictamen (informe final de auditoría), lo cual se puede hacer de dos maneras, ya sea en forma directa a través de una reunión ejecutiva con los directivos de la empresa, o por envío formal del dictamen final de la auditoría al directivo mayor de la organización. Éste ya es el informe final de la auditoría practicada y, por lo tanto, no se debe admitir ningún comentario adicional que pudiera modificar lo ahí presentado, ya que es el producto final de la auditoría y, por lo tanto, ya no cabe ninguna alteración al mismo. De hacerlo sería tanto como crear expectativas de duda sobre la veracidad y confiabilidad de su contenido.

4.3 Características del informe de auditoría.

El informe final de la auditoría de sistemas de información debe tener dos características fundamentales, las cuales son:

Características de fondo. Las características de fondo se refieren al contenido impecable del informe, por lo tanto el auditor debe tomar en cuenta los siguientes aspectos:

- La información que contiene el documento debe ser veraz, confiable, oportuna y sin alteraciones.
- La terminología debe ser exacta y objetiva.

- El contenido del informe debe ser congruente con lo observado, sin inventar, distorsionar o modificar lo encontrado en la evaluación.
- El contenido debe abarcar todo lo que se debe informar de los sistemas auditados sin abundar en explicaciones inútiles.
- El lector debe captar inmediatamente la problemática que reporta el auditor así como la opinión que plasma respecto a los sistemas de información auditados.

Características de forma. Las características de forma se refieren a la presentación del informe, por lo tanto el auditor debe tomar en cuenta los siguientes aspectos:

- El informe debe estar redactado en forma concisa, clara, sencilla y amena.
- Se deben evitar entorpecedores de lectura (redundancia, repeticiones y reiteraciones).
- La forma de presentar el informe debe ser profesional (por computadora e impecable).
- Su redacción debe ser impecable en cuanto a ortografía y puntuación, en estilo impersonal y sin ningún error en la forma de presentarlo.

Cabe aclarar que el informe final de auditoría debe contar con las dos características antes mencionadas, ya que la falta de alguna de ellas traería como consecuencia un informe sin presentación y de contenido irreal.

4.4 Estructura del informe de auditoría.

El informe de auditoría debe contener los siguientes puntos:

Oficio de presentación. Es un documento de carácter oficial que sirve como presentación del informe, mediante este documento se pone a consideración de los directivos de la empresa el resultado de la auditoría practicada. Este documento debe contener los siguientes puntos: logotipo y nombre de la empresa auditora, fecha del informe, funcionario que recibe el informe, empresa y área auditada, período de evaluación, nombre, firma y cargo del responsable. Véase Ilustración 27.

Introducción. Es la parte del informe donde el responsable de la auditoría hace la presentación formal de su trabajo, en este apartado se manifiesta el objetivo de la auditoría, las razones que motivaron a llevarla acabo y, si es el caso, los fundamentos que apoyen su realización, en algunas ocasiones también se puede indicar la metodología y las herramientas utilizadas en la evaluación de los sistemas de información, aunque esto último no es forzoso.

Dictamen de la auditoría. Este es un documento de carácter formal que plasma la opinión profesional del auditor respecto al comportamiento de los sistemas de información. Evidentemente, el dictamen está apoyado por la experiencia y conocimientos del auditor, así como en la confianza del uso de las herramientas e instrumentos apropiados. Este documento contiene los siguientes puntos: logotipo de identificación, nombre de la empresa y área auditada, fecha de emisión del dictamen, ejecutivo receptor del dictamen, breve introducción al dictamen, contenido del informe de auditoría, dictamen y recomendaciones del auditor, responsable de emitir el dictamen. Véase Ilustración 28.

Situaciones detectadas. Este documento es un formato especial para la recopilación de situaciones o desviaciones encontradas, el cual está formado por una serie de hojas, en las cuales el auditor anota en manuscrito o tipografía todas las desviaciones que encuentra durante su evaluación. Véase Ilustración 29.

Situaciones relevantes. Este documento es una réplica simplificada del formato anterior, solo que en este último se anotan las situaciones consideradas como relevantes. Es recomendable que las situaciones relevantes incluidas en este documento sean las mismas que se establecieron en el documento anterior, incluso con las mismas palabras, pero en este formato no deben aparecer a mano sino mecanografiadas. Este formato se anexa para posibles aclaraciones y consultas de las desviaciones que se reportan en el dictamen. Véase Ilustración 30.

Anexos. Cuadros, estadísticas, actas o cualquier otro documento que sirva de soporte para reafirmar las desviaciones presentadas. Los anexos son incluidos para que el auditor cuente con una herramienta de apoyo gráfica.

Confirmaciones en papeles de trabajo. Este documento no se debe integrar al informe final de la auditoría, sin embargo, al presentar el informe a los directivos, es conveniente que el auditor tenga a la mano el legajo de papeles de trabajo, ya que podría necesitar hacer aclaraciones importantes de lo reportado, entonces puede recurrir a las pruebas documentadas. De ahí la importancia de llevarlo.

Ciudad de México, __ de_____de____.

AUDITORÍA EN SISTEMAS A.C.

Lic.
Director General.
Presente.

Con un saludo me dirijo a usted, de la manera más atenta con el fin de presentarle el Informe de Resultados de la auditoría practicada al área de _____ de la empresa _____**,** la cual se realizo del ___ de_____ al ___ de _____ del _____**.**

CONTENIDO O CUERPO DEL OFICIO
(Dar una breve descripción de los puntos que fueron evaluados y de los aspectos que integran el informe)

Nombre, cargo y firma del
responsable de emitir el informe

Ilustración 1. Formato de oficio de presentación.

Ciudad de México, __ de_____de____.

AUDITORÍA EN SISTEMAS A.C.

Lic.
Director General.
Presente.

De acuerdo con las instrucciones giradas por el consejo de administración de la empresa a su digno cargo, me dirijo a usted, de la manera más atenta con el fin de presentarle el dictamen de la auditoría practicada al área de _____ de la empresa _____**,** la cual se realizo del ___ de_____ al ___ de _____ del _____**.**

De los resultados obtenidos durante la evaluación me permito informarle las siguientes observaciones:

CONTENIDO DEL INFORME DE AUDITORÍA
(Resumir el diagnostico del resultado de la auditoría)

OPINIÓN Y RECOMENDACIONES DEL AUDITOR

Nombre, cargo y firma del
responsable de emitir el informe

Ilustración 2. Formato de Dictamen de la auditoría.

EMPRESA: _____.

AREA AUDITADA: _____.

DÍA	MES	AÑO

Ref.	Situaciones	Causas	Solución	Fecha de solución	Responsable

Elaboró (Nombre y firma): _____

Aprobó (Nombre y firma): _____

Ilustración 3. Formato de situaciones encontradas.

EMPRESA: _____.

AREA AUDITADA: _____.

DÍA	MES	AÑO

Ref.	Situaciones	Causas	Solución

Elaboró (Nombre y firma) _____

Aprobó (Nombre y firma) _____

Ilustración 4. Formato de situaciones relevantes.

CONCLUSIONES

1. Generalmente el personal piensa que cuando se hace una auditoría en la organización, es porque ya se encontraron fallas, y por lo tanto se deberán encontrar a los responsables de éstas. Esta idea es absurda debido a que la auditoría no puede encontrar errores antes de llevarse acabo, además el sentido de la auditoría es más amplio ya que ésta realiza un examen con el propósito de evaluar la eficiencia y eficacia con que se está operando, esto es con la finalidad de determinar si la información es fiable y veraz, y en caso de encontrar fallas dotará a la organización de las herramientas necesarias que le permitan mejorar y lograr sus objetivos, por lo tanto el personal auditado de la organización debe tomar a la auditoría como una evaluación, no como un cacería para cortar sus cabezas.

2. Es importante destacar que la auditoría en informática es una disciplina nueva, producto del desarrollo de la informática, esta nueva disciplina evalúa la información desde su generación hasta su utilización, considerando su seguridad y confidencialidad de la misma, con el propósito de conseguir el mejor uso de la información al menor costo, evitando su duplicidad.

3. En cuanto al trabajo de auditoría, se requiere que el auditor conozca no sólo sobre las materias que le son propias, sino que tenga conocimientos acerca del área de sistemas e informática, además el auditor debe ser un profesional serio, capaz y responsable, ya que una auditoría mal hecha puede acarrear consecuencias drásticas para la organización auditada, principalmente económicas.

4. Los sistemas de información se han convertido en una herramienta de mucho valor para las organizaciones, ya que intervienen en la toma de decisiones de la misma, por lo tanto es importante que éstos se sometan a un control estricto de evaluación.

5. Se puede decir que la importancia de la auditoría de sistemas radica en optimizar el buen desempeño de los sistemas de información, ya que esta proporciona los controles necesarios que permiten a los sistemas ser confiables y gozar de un alto nivel de seguridad.

6. La evaluación de los sistemas busca comprobar que la aplicación cumpla las especificaciones requeridas por el usuario, que se haya desarrollado dentro de lo presupuestado y que efectivamente cumpla con lo objetivos y beneficios esperados.

7. Para realizar una auditoría de sistemas de información se debe diseñar una metodología específica, que muestre de forma concreta cada uno de los pasos que se deben seguir para llevar acabo la evaluación, de tal forma que no se omita ninguna actividad de la auditoría.

8. La planeación es un punto muy importante en la evaluación de los sistemas de información, ya que de ésta depende el éxito de la auditoría, debido a que controla todas las actividades, métodos, técnicas, y procedimientos para llevarla acabo, además se encarga de elaborar los documentos y presupuestos necesarios para su ejecución.

9. Los sistemas de información deben ser evaluados de acuerdo con el ciclo de vida del desarrollo que normalmente siguen, pero además deberán evaluarse en la ejecución, en su impacto, en su economía y de forma subjetiva.

10. Cabe destacar que el verdadero trabajo del auditor, es reportar las desviaciones que encontró durante su evaluación, encontrar las causas que originaron dichas desviaciones y acordar las posibles soluciones conjuntamente con el auditado, lo anterior es la verdadera función de la auditoría de sistemas de información.

11. El auditor solo puede emitir un juicio global o parcial basándose en hechos y situaciones encontradas, pero carece de poder para modificar la situación que ha analizado y evaluado.

12. La auditoría no debe terminar cuando el auditor presenta el informe final a los directivos de la empresa, sino todo lo contrario, esta entrega marca el comienzo de una serie de auditorias y revisiones periódicas, con el propósito de tener un adecuado seguimiento de las situaciones encontradas para lograr las correcciones a los problemas y las mejoras a los sistemas que lo ameriten.

13. Yo recomiendo que la auditoría de sistemas de información se realice cuando se presenten las siguientes condiciones:

- El sistema o los sistemas de información no trabajan de forma correcta.
- No cumple con los requisitos del usuario.
- La información que reporta el sistema o los sistemas de información no es la adecuada, es decir, dicha información no es confiable, veraz y oportuna.
- O simplemente como una revisión periódica.

14. ¿La auditoría informática es o no necesaria? Desde mi punto de vista la auditoría informática, ya sea de sistemas de información, de comunicaciones, de seguridad o de cualquier otra área de la informática es necesaria ya que ésta auxilia a la informática, debido a que es un área bastante amplia, por lo tanto la auditoría informática se convierte en una función importante de la informática.

BIBLIOGRAFÍA

Análisis y diseño de sistemas de información.
SEEN, James.
Editorial Mc Graw Hill.

Análisis y Diseño de Sistemas.
KENDALL, Keneth.
Editorial Prentice Hall.

Auditoría en informática.
ECHENIQUE GARCÍA, José Antonio.
Editorial Mc Graw Hill.

Auditoría en informática, un enfoque práctico.
Mario G. Piattini, Emilio del Peso.
Editorial Ra-Ma.

Computación & Informática Hoy.
BEEKMAN, George.
Editorial Addison–Wesley Iberoamericana.

Auditoría en centros de cómputo.
L.I. David H.
Editorial Trillas.

Auditoría en Sistemas Computacionales.
Muñoz Razo, Carlos.
Editorial Pearson Education.

Reingeniería de la auditoría en informática.
Solís Montes, Gustavo Adolfo.
Editorial Trillas.

Auditoría en informática.
Hernández Hernández, Enrique.
Editorial CECSA.

Auditoría informática.
Rivas, Gonzalo Alonso.
Editorial DIAZ DE SANTOS, S.A.

Técnicas de la auditoría en informática.
Yann Derrien.
Editorial Alfaomega Marcombo.

Diseño de sistemas de información, teoría y práctica.
Burch, Grudnitski.
Editorial LIMUSA, Noriega Editores.

Sistemas de información basados en computadoras, para la administración moderna.
Robert G. Murdick, Joel E. Ross.
Editorial Diana.

Principios básicos de auditoria.
Holmes, Arthur.
Editorial CECSA.

Administración de la función informática.
Hernández, Jiménez, Ricardo.
Editorial Trillas.