UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

AUDITORIA EN INFORMATICA

SEMINARIO DE INVESTIGACION CONTABLE

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN CONTADURIA

P R E S E N T A :

GEORGINA VIRGEN GOMEZ MARQUEZ

ASESOR DEL SEMINARIO:

C.P. Y MBA. JOSE ANTONIO ECHENIQUE GARCIA

MEXICO, D.F. 1998

A MIS PADRES

AGRADEZCO A MIS QUERIDOS PADRES POR HABERME DADO LA VIDA Y LA OPORTUNIDAD DE REALIZARME COMO PROFESIONISTA Y COMO MUJER Y DEJARME LA MEJOR DE LAS HERENCIAS QUE SON LOS ESTUDIOS.

DIOS LOS BENDIGA.

A MI ESPOSO Y A MIS HIJOS

POR SU COMPRENSIÓN Y APOYO Y SOBRETODO POR SU SACRIFICIO PARA IMPULSARME A SEGUIR ADELANTE.

LOS AMO.

A LA MÁXIMA CASA DE ESTUDIOS LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO Y A LA HEROICA FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN, GRACIAS POR LA OPORTUNIDAD QUE ME OFRECIERON PARA OBTENER UN COMPROMISO CON ELLAS MISMAS Y CON LA SOCIEDAD.

CON ORGULLO, ADMIRACIÓN Y RESPETO.

C.P. Y MBA. JOSÉ ANTONIO ECHENIQUE GARCÍA.

AGRADEZCO INFINITAMENTE POR LA OPORTUNIDAD, SUS CONOCIMIENTOS, APOYO Y TIEMPO PARA CULMINAR ESTE OBJETIVO.

PROFESOR MIL GRACIAS.

I N D I C E

PAG.

A N T E C E D E N T E S

En años anteriores observamos como la informática ha apoyado sistemáticamente para la solución de los problemas económicos, sociales y políticos, así como la información para la toma de decisiones por la alta dirección provocando una acción para la estabilidad del organismo y el cumplimiento de los objetivos del control interno.

En la actualidad se ha comprobado el mal uso de la información que personal no autorizado, ha llegado al extremo de ocasionar fraudes significativos que han dañado los intereses del organismo.

Para evitar el mal uso de información ha sido necesario crear controles que permitan generar información objetivamente y es precisamente la tarea que le corresponde a la auditoria de informática, vigilar el cumplimiento de éstos.

I N T R O D U C C I Ó N

Es un trabajo de investigación que expresa en su contenido temas que son de importancia para el auditor de sistemas de información.

En el capítulo 1 se habla de las generalidades de la auditoría y de la informática así como el desarrollo que han manifestado.

El capítulo 2 analiza los elementos del control interno sujetos al estudio y evaluación de los controles de los sistemas de información, asimismo trata puntos relevantes para la seguridad de la información, dando pauta a técnicas para la auditoría de sistemas.

El capítulo 3 indica la importancia que tiene la intervención del auditor en informática en el desarrollo de los sistemas de información, se consideran los aspectos más relevantes como producto final de cada etapa del desarrollo de sistemas.

Este trabajo muestra la importancia que tienen los controles generales en una auditoría de sistemas de información.

O B J E T I V O

El objetivo de esta investigación es contribuir con conocimientos básicos para capacitar al auditor en el estudio y evaluación de los sistemas de información con el fin de realizar adecuaciones, para que sean sistemas auditables.

1. CONCEPTOS DE AUDITORIA Y DE INFORMÁTICA.

En este capítulo se define el concepto de Auditoría Informática y las normas que le son aplicables, se hablará del desarrollo que la función ha tenido y los tipos de auditoría informática que pueden realizarse; distinguiendo al profesional o profesionales que pueden ejecutar esta función y cuál es su participación.

Para ello previamente se definirán otros conceptos que le son relativos como la auditoría convencional y sus normas, se mencionará la evolución de la función, los tipos de auditoría que se han desarrollado derivado de las características de la revisión, asimismo se hablará de otros conceptos relativos a la informática y la evolución de la informática para llegar a un nivel de apoyo a la administración, para que con estos conceptos se comprendan las definiciones que son objeto de este capítulo.

1.1 CONCEPTOS DE AUDITORIA.

1.1.1 DEFINICIÓN DE AUDITORIA.

El término auditoría es muy antiguo y en su forma más simple implica el acto de revisar.

De la definición del diccionario de la lengua española, Larousse, se define: " El examen de las operaciones financieras, administrativas y de otro tipo de una entidad pública o de una empresa por especialistas ajenos a ellas y con objeto de evaluar la situación de las mismas "[1]

El boletín C de normas de auditoría del Instituto Mexicano de Contadores Públicos dice[2]:

" La auditoría es una actividad profesional. En este sentido implica, al mismo tiempo, el ejercicio de una técnica especializada y la aceptación de una responsabilidad pública. Como profesional, el auditor desempeña sus labores mediante la aplicación de una serie de conocimientos especializados que vienen a formar el cuerpo técnico de su actividad; sin embargo, en el desempeño de esa labor, el auditor adquiere responsabilidad, no solamente con la persona que directamente contrata sus servicios, sino con un vasto número de personas, desconocidas para él que van a utilizar el resultado de su trabajo como base para tomar decisiones de negocios o de inversión ".

---

[1] *Larousse, Diccionario de la Lengua Española, tomo 1.*
[2] I.M.C.P., Normas y Procedimientos de Auditoría.

Por lo tanto, se habla de la utilización de una técnica especializada que vienen siendo los mismos conocimientos adquiridos en la profesión para ser efectuados con alto nivel de calidad además implica adquirir responsabilidades sociales, éticas y morales debido a que el resultado de este trabajo será utilizado para la toma de decisiones en la empresa auditada.

Es importante señalar que la auditoría no detecta fallas y errores únicamente sino que evalúa la eficiencia y eficacia de una empresa para señalar alternativas para corregir o mejorar lo existente.

Se definen los conceptos de eficiencia y eficacia para mejor comprensión.

Eficiencia.- " Relación existente entre el trabajo desarrollado, el tiempo invertido, la inversión realizada en hacer algo y el resultado logrado."[3]

Eficacia.- " Virtud, actividad o poder para obrar. Capacidad para producir un efecto. Aptitud."[4]

De los puntos anteriores se define la auditoría para efectos de esta investigación:

La auditoría es una actividad profesional que implica el ejercicio de técnicas y procedimientos especializados aplicables al tipo de revisión que deberá efectuarse con el objeto de evaluar y mejorar lo existente, detectar y corregir errores y proponer alternativas de solución en un informe como resultado del trabajo obtenido que sirva como base para la toma de decisiones.

Normas de auditoría.

Después de haber hablado sobre la auditoría, es necesario hablar sobre la realización de un trabajo de auditoría, en donde se adquieren responsabilidades sociales, éticas y legales ya que el resultado de su trabajo será utilizado por la empresa examinada para diferentes fines de terceros.

Para que la auditoría tenga un alto nivel de calidad debe basar su trabajo en fundamentos llamados " Normas de Auditoría ".

El boletín A de normas de auditoría del Instituto Mexicano de Contadores Públicos, las conceptualiza como los " requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña y a la información que rinde como resultado

[3] Larousse, Diccionario de la Lengua Española, tomo 1.
[4] *Diccionario Porrúa de la Lengua Española.*

de dicho trabajo "[5] .

Se clasifican en:

a) Normas Personales
b) Normas de Ejecución del Trabajo
c) Normas de Información

a) Normas Personales.

Se refieren a las cualidades que debe reunir la persona en sí del auditor para poder dedicarse a la realización de la auditoría.

Entrenamiento técnico y capacidad profesional.

La persona que ofrezca sus servicios para el desempeño de una actividad profesional, deberá haber cumplido con los requisitos establecidos en las instituciones para la obtención del título profesional de la carrera de Licenciado en Contaduría, de ésta manera adquirir el entrenamiento técnico y capacidad profesional como auditor.

Cuidado y diligencia profesional.

Debemos poner mayor cuidado y diligencia profesional al realizar un trabajo de auditoría en la preparación de informe o dictamen.

Independencia.

Consiste en la objetividad del trabajo sin dejarnos influir en consideraciones subjetivas.

b) Normas de ejecución del trabajo.

Planeación y supervisión.

La adecuada planeación del trabajo de auditoría implica preveer en forma anticipada los procedimientos de auditoría y el personal que deberá emplearse, sin perder de vista la supervisión del personal y del trabajo desarrollado oportunamente.

Estudio y Evaluación del Control Interno.

Consiste básicamente en efectuar un estudio y evaluación adecuados de control existente, que sirva de base para determinar el grado de confianza en él; asimismo, que permita determinar la

[5] *I.M.C.P., Normas y Procedimientos de Auditoría.*

naturaleza, extensión y oportunidad que va a dar a los procedimientos de auditoría.

Obtención de evidencia suficiente y competente.

El auditor debe obtener evidencia comprobatoria que realmente sirva para justificar la opinión y competente en el grado en que la
evidencia debe circunscribirse a aquellos aspectos que tienen influencia en el juicio y la opinión.

c) Normas de Información.

El resultado final del trabajo del auditor es su dictamen o informe. Mediante éste se pone en conocimiento de las personas interesadas los resultados del trabajo de auditoría y la opinión que se ha formado a través de la revisión y en muchos casos, es la única parte, de dicho trabajo que queda a su alcance.

1.1.2 EVOLUCIÓN DE AUDITORIA.

Ahora bien, veremos el desarrollo evolutivo que el área de auditoría ha observado en un período de aproximadamente 50 años hasta llegar a un nivel de apoyo directo al Consejo de Administración, de la siguiente manera:

- En la década de los 40's se identificaba a la Auditoría Interna como un área incipiente y primitiva que dependía del contador realizando actividades de conciliación de partidas, análisis de cuentas, y corroborar documentos y su registro.

- En la década de los 60's y a la luz de los logros obtenidos y potenciales, el área de contraloría hace depender de sí la labor de Auditoría.

- Hacia la década de los 70's las direcciones financieras conscientes de la importancia de sus resultados, nuevamente la hacen emigrar y depender de ellas.

- A partir de los 80's en las empresas vanguardistas, se aprecia la tendencia de llevar a depender a Auditoría de la Dirección General y en algunos casos del propio Consejo de Administración.

El impacto de la función ha sido tal que en el sector público ha merecido el reconocimiento y la estructuración para constituirse en Secretaría de Estado, con atribuciones de mayor preponderancia para el cumplimiento de algunos de los postulados del Gobierno de la República.

1.1.3 TIPOS DE AUDITORIA.

Para iniciar el presente estudio, se tomarán dos formas básicas para clasificar los tipos de auditoría.

Por quien las realiza y

Por los objetivos que se persiguen

Por quien las realiza puede ser de dos formas:

Auditoría Externa: Es aquella revisión y evaluación que realiza un auditor o grupo de auditores ajenos completamente a la organización en donde se efectúa su trabajo.

Auditoría Interna: Es aquella revisión y evaluación que realiza un auditor o grupo de auditores empleados formalmente por la organización, pero sus funciones y su actuación, son ajenas totalmente a la operación de ésta.

Por los objetivos que se persiguen, la auditoría puede ser:

Auditoría Financiera: El objetivo es rendir una opinión profesional independiente sobre la razonabilidad con que los estados financieros presentan la situación financiera y los resultados de las operaciones de la organización de acuerdo con los principios de contabilidad, aplicados sobre bases consistentes.

Auditoría Operacional: El servicio que presta el contador público cuando examina ciertos aspectos administrativos, con la intención de hacer recomendaciones para incrementar la eficiencia operativa de la entidad.

Auditoría Administrativa: Examina estructuras, objetivos, funciones, planes, políticas y propósitos de operación, evaluando el adecuado aprovechamiento de sus recursos humanos, materiales y técnicos, puede abarcar una función específica; o bien, se le puede dar un enfoque de sistema y puede abarcar una unidad o grupo de unidades que forman un organismo social.

Auditoría Integral: Es un servicio útil y oportuno para la administración de la entidad, debe estar presente en cada una de las etapas del proceso administrativo como elemento de supervisión para determinar carencia de objetivos y políticas, ineficiencias, carencia de coordinación, duplicidad de funciones y controles, puede seccionarse departamentalmente y realizarse en ciertos periodos, la puede desarrollar un profesional no necesariamente un licenciado en contaduría, la cual culmina con un informe para la alta dirección encaminado hacia la toma de decisiones.

De los tipos de auditoría antes mencionados podemos efectuar una revisión que cumpla con la prestación de un servicio de asistencia constructiva a la administración con el propósito de mejorar la conducción de las operaciones y sistemas para obtener un mayor beneficio económico para la empresa.

1.2. CONCEPTOS DE INFORMÁTICA.

1.2.1 DEFINICIÓN DE INFORMÁTICA.

Para la definición de Informática se tomará como base la diferencia que existe entre el dato y la información, la cual se expone en los siguientes términos:

El dato puede ser un número, letras, símbolos o hechos que describen un objeto, idea, condición, situación u otro factor, mientras que la información le da un significado a los datos en forma clasificada y ordenada con un objetivo común.

Por lo tanto, se puede decir que los datos son elementos básicos de la información, sin ellos no hay información.

La información debe ser oportuna, clara, verídica, confiable dirigida a los altos mandos para la toma de decisiones.

De esta manera, ya se tienen fundamentos para emitir una definición de informática como sigue:

Una disciplina que clasifica y ordena datos dado un hecho, por medios mecánicos, manuales , electromecánicos, electrónicos, generando información, confiable, verídica, oportuna, presentados en algún medio, papel, pantalla, medios magnéticos, que deberá contener el significado de los datos y/o símbolos una vez procesados por cualquier medio, para ser transmitida por canales eficientes y finalmente presentada para apoyar en la toma de decisiones.

De la definición anterior se deriva que la informática puede usar los equipos electrónicos como una de sus herramientas.

1.2.2 EVOLUCIÓN DE INFORMÁTICA.

Se hablará del desarrollo de ésta función desde el nivel operativo hasta el nivel de apoyo a la Dirección General en un periodo de aproximadamente 40 años, de la siguiente manera:

- El surgimiento y comercialización de la primera generación de computadoras se inició en la década de los 50's.

Impacto: Transformó substancialmente los mecanismos administrativos, reducción de tiempos horas-hombre.

- En la década de los 60's al surgir la 2a. generación de computadoras se logró un mayor desarrollo de los sistemas administrativos y operativos de información.

Impacto: Origina un mayor crecimiento y proliferación de sistemas y una mayor demanda de nuevas capacidades y recursos tecnológicos

- Durante la década de los 70's con la 3a. generación de computadoras dan inicio los sistemas en línea y al uso de bases de datos.

A fines de ésta década, hacen su aparición las Computadoras Personales.

Impacto: Los sistemas se hacen indispensables sobre todo en empresas donde se manejan grandes volúmenes de información, y esta información debe ser precisa, oportuna, verídica y confiable.

Lo cual nos indica un avance en la cultura informática, pues la incorporación de las computadoras personales no es solo en empresas sino también en los hogares.

- En los 80's con mejoras incorporadas a las computadoras, surge con un nuevo recurso el software denominado de 4a. generación, permitiendo contar con sistemas desarrolladores de aplicaciones orientados a sustituir los superlenguajes y con ello la labor misma del programador.

Impacto: Los sistemas se van convirtiendo en la estrategia misma del negocio, ahora los altos funcionarios ya tienen la cultura informática que les hacía falta en décadas anteriores y ellos mismos ya pueden exigir aún más a los sistemas por lo que ya entran en sus planes.

La situación descrita ha sido factor determinante de la evolución informática en las empresas, destacando los siguientes hechos:

- En la década de los 50's, la función denominada " PED " dependía normalmente del área contable-financiero apoyándolo con sistemas operativos tradicionales como el registro de operaciones, control de inventarios y nómina, por lo que cualquier sistema estaba dentro del rango operativo de la organización.

- En la siguiente década los 60's, la Contraloría se percata de la importancia de PED y hace depender a esta área directamente de

ella. En este momento PED depende de una sola área.

- Durante los 70's las áreas de Dirección conscientes de la capacidad y apoyo que representa la función de PE - la cual empieza a denominarse Informática - hacen escalar nuevas posiciones haciéndola depender directamente de ellas. Se provoca una descentralización de la función de PE alcanzando niveles directivos.

- A partir de los 80's en las empresas vanguardistas se observa una marcada tendencia a hacer depender a la función informática de la Dirección General debido a que en esta función se encuentra la posibilidad de planeación táctica y estratégica aunados a los de servicio y control de la organización; así como coordinar y dirigir las acciones para alcanzar algún objetivo apoyándose con la combinación de los medios disponibles para alcanzar ese fin.

- En los 90's se utilizan los sistemas basados en conocimientos del hombre que junto con su experiencia son almacenados electrónicamente para ser manejados de una manera activa y utilizados para la obtención de nuevos conocimientos y solución de problemas.

Impacto: Se espera que las futuras aplicaciones sean desarrolladas por usuarios finales y gerentes no profesionales de sistemas de información.

Por este motivo que se les está proporcionando a los desarrolladores de sistemas el " ambiente de desarrollo de aplicaciones " como herramientas que permitan desarrollar sistemas.

Es así como en tan sólo 40 años la función informática ha pasado a un área incipiente de bajo nivel a colocarse en un primer plano en la estructura organizacional de las empresas.

1.3 AUDITORIA INFORMÁTICA

1.3.1 DEFINICIÓN DE AUDITORIA INFORMÁTICA.

Para la definición de Auditoría Informática, se cita la siguiente, del Lic. J. Antonio Echenique.

" Auditoría en informática es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de

la información que servirá para una adecuada toma de decisiones"[6]

Tomando como base el párrafo anterior a continuación se dará la definición para efectos de esta investigación:

Auditoría Informática es una actividad profesional especializada apoyada en técnicas y procedimientos para revisar, evaluar y supervisar cada uno de los procesos que generan información desde su inicio hasta su término, así como también establece y evalúa los controles de acuerdo a los objetivos y políticas de la empresa, considerando al mismo tiempo los aspectos funcionales y organizacionales de quienes desarrollan la actividad informática, sin perder de vista la evaluación técnica de los recursos, para que al finalizar su actividad, se emita un informe sobre las carencias detectadas que se presentará a la Dirección.

Normas de auditoría informática.

Al igual que en la realización de la auditoría financiera, se adquieren responsabilidades al efectuar una auditoría en informática, tanto sociales, y éticas como legales ya que el resultado final obtenido servirá para la toma de decisiones.

Por lo tanto, la auditoría informática también debe tener un alto grado de calidad por lo que se determinarán las normas de auditoría informática para los fines de este trabajo.

a) Normas personales.

Entrenamiento técnico y capacidad profesional.

El entrenamiento técnico se adquiere con los conocimientos adquiridos sobre la informática, como una disciplina de alta especialización técnica y acelerado desarrollo tecnológico lo que hace necesario que el auditor en informática se mantenga actualizado en cuanto a desarrollo tecnológico.

Cuidado y diligencia profesionales.

El auditor está obligado a ejercitar cuidado y diligencia razonables en su revisión a los aspectos informáticos significativos y a la preparación de su informe.

Independencia

El auditor en auditoría informática, será independiente del área o sistema que revise a fin de lograr la terminación de su

[6]Echenique, G. José A. Auditoría en Informática.

trabajo en forma objetiva sin permitir opiniones subjetivas.

Planeación y supervisión.

El auditor en informática debe preveer la auditoría desde su inicio hasta su terminación procurando al mismo tiempo la supervisión en el desarrollo de la auditoría en informática.

b) Normas de ejecución del trabajo.

De las cuales observamos la exigencia del cumplimiento en su carácter de obligatorio así como para todas las normas de auditoría, del cuidado y diligencia que son fundamentales en la ejecución del trabajo, desde la planeación hasta la documentación que le permita fundamentar su opinión.

Estudio y evaluación del control interno.

Básicamente es efectuar un estudio y evaluación adecuados del control interno en los siguientes aspectos:

- Estructura orgánica del departamento
- Funciones del personal
- Revisión a todas las aplicaciones incorporadas al computador
- Revisión al sistema en su totalidad, fases manuales y computarizadas.
- Realizar pruebas de auditoría a los sistemas (pruebas de cumplimiento)
- Revisar las instalaciones de los equipos

Evidencia suficiente y competente.

La información que obtenga el auditor en gran parte será emitida por un computador, así como reportes obtenidos por las pruebas efectuadas a los programas o bien reportes que indiquen errores en sistemas en producción, que será la evidencia comprobatoria y competente que permitirá apoyar su opinión en forma objetiva.

c) Normas de información.

Estas normas son relativas al informe como resultado final del trabajo de auditoría en informática para dar a conocer a los interesados los resultados de supervisión, conclusiones y posibles soluciones.

1.3.2. EVOLUCIÓN DE LA AUDITORIA INFORMÁTICA.

Las primeras auditorías que se realizaban, utilizaban procedimientos tradicionales de auditoría en donde verificaban

manualmente el comportamiento y validez de las transacciones económicas y financieras, en el caso de tener un sistema de información automatizado únicamente se utilizaban procedimientos externos al computador, en donde solamente se puede determinar la confiabilidad de los datos de entrada y resultados obtenidos con la desventaja de desconocer la validéz de su procesamiento.

Estas auditorías son conocidas como " **Auditoría sin la computadora** "

Las siguientes auditorías comenzaron a utilizar los recursos de cómputo y los archivos magnéticos de una organización con el fin de automatizar procedimientos de auditoría para determinar la evaluación, verificación, análisis e interpretación de la información auditada, es en este momento en donde el auditor usuario en un plano de revisor y certificador de registros manuales pasa a plano interpretativo y de análisis del comportamiento de los datos.

La utilización de los recursos de cómputo por el auditor le permite:

Verificar las cifras totales y cálculos para comprobar la exactitud de los reportes de salida producidos por la computadora.

Seleccionar datos mediante técnicas de muestreo.

Utilizar paquetes de auditoría.

Supervisar la elaboración de programas de auditoría.

Revisar las aplicaciones significativas incorporadas al computador.

Revisar el sistema en su totalidad, tanto las fases manuales como computarizadas.

Revisar el control interno general de la instalación del equipo de cómputo.

Realizar pruebas de auditoría a los sistemas.

Para la automatización de los procedimientos de revisión, el auditor se vale del software denominado **Paquetes de Auditoría,** en este avance además de los paquetes el auditor ya puede contar con sus propios procesos con ayuda de otros sistemas, o bien técnicas de auditoría asistidas por computadora.

Se mencionarán los procedimientos específicos de auditoría del computador.

Los procedimientos específicos de auditoría del computador comprenden el uso de variadas técnicas que permiten al auditor realizar pruebas en un ambiente de PE, dichas técnicas se pueden dividir en dos grandes grupos:

Técnicas para realizar pruebas de cumplimiento y

Pruebas sustantivas.

Técnicas para realizar pruebas de cumplimiento.

Las cuales se aplican para revisar el cumplimiento del control interno establecido por lo que las pruebas están enfocadas a confirmar que los programas y controles de la empresa funcionan con las estipulaciones técnicas bajo las cuales fueron diseñados.

Dentro de estas técnicas se definen las siguientes:

Lote de datos de prueba.- La preparación de datos de entrada al computador que le presenten un repertorio de transacciones reales procesadas mediante el programa usado en el desarrollo normal de los procesos, con el propósito de identificar resultados predeterminados.

Datos de prueba integrados.- Con esta técnica se obtiene una razonable certeza de que las transacciones reales y las pruebas del auditor son procesados con el mismo programa y sujetas ambas a los mismos controles contables internos.

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

Simulación.- Consiste en la formulación por el auditor de su propio programa para realizar el mismo proceso que efectúa el programa real y utilizar la misma información real para comparar los resultados.

Revisiones de acceso.- Se conserva un registro computarizado de todos los accesos a determinados archivos.

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

Pruebas sustantivas.

Las técnicas adecuadas para el auditor en la comprobación y validéz de la información aprovechando el computador para verificar el contenido y corrección de los archivos mantenidos en medios magnéticos de computadores.

Dentro de estas técnicas se definen las siguientes:

Programas especiales.- El auditor elabora sus propios programas para procesar cierta información contenida en los archivos del computador.

Paquetes de auditoría.- Es un conjunto de programas que permite al auditor aplicar una serie de técnicas para verificar controles internos en los sistemas sobre todo, para extraer y procesar información de los archivos con mayor facilidad.

El auditor que intervenga en estas revisiones debe tener conocimientos del diseño conceptual de las aplicaciones, de la descripción y organización de los datos, de las etapas del proceso de datos y del ambiente en que operan y además conocimientos y experiencia en la labor de auditoría que le permitan tener una comprensión adecuada del trabajo que esta realizando, por lo que para automatizar los procedimientos tradicionales de auditoría, es necesario capacitar a todos los auditores para apoyarse en estas técnicas informáticas.

En conclusión se desarrolla un conjunto de técnicas y procedimientos que aplicados en un medio ambiente de Procesamiento Electrónico de Datos (PE), proporcionan al auditor los elementos de juicio suficientes para depositar su confianza en la información procesada y contenida en los registros contables, almacenados en dispositivos magnéticos o impresos en listados emitidos por un computador.

Estas auditorías son conocidas como " **Auditoría con la computadora** " .

De la existencia de sistemas de información computarizados en las organizaciones a todos los niveles y tratándose de información para la toma de decisiones, se considera la información como un activo de la empresa y uno de los objetivos del control interno es precisamente la salvaguarda de los activos, de aquíi nace la necesidad de efectuar auditorías para verificar el control en las áreas que utilizan los medios electrónicos generadores de esta información.

De las necesidades arriba mencionadas, efectivamente se debe realizar una auditoría que supervice la generación de esta información, con la finalidad de identificar, evaluar y verificar el cumplimiento del control interno de cada uno de los elementos que intervienen en este proceso, desde la Gerencia hasta el último nivel de apoyo a la Gerencia de PE.

Lo cual incluye una revisión al equipo, a las instalaciones en general, los programas, la operación del sistema, asignaciones de equipos, funciones del personal, etc.; para que después de esta evaluación se emita un informe que sirva de base para la toma de decisiones.

A esta auditoría que pretende una revisión general, en este caso al departamento de PE, se le llama Auditoría Integral, la cual debe hacerse bajo los principios (normas de auditoría) y ética profesional de la auditoría tradicional, dirigidos al criterio de supervisión.

1.3.3. QUIEN DEBE EFECTUAR LA AUDITORIA EN INFORMÁTICA ?

Las revisiones que dieron inicio a la función de auditoría, consistieron en la aplicación de normas y procedimientos tradicionales que le son relativos para comprobar y verificar la información contenida en los estados financieros, revisando los registros contables elaborados manualmente por la empresa auditada, asi mismo el auditor elaboraba sus papeles de trabajo y cálculos manuales.

Las auditorías que continuaron se efectuaban en empresas que contaban con sistemas de información computarizados, en donde se aplicaban los procedimientos tradicionales de auditoría siendo estos externos al computador porque se continuaba verificando manualmente el comportamiento y validéz de la información financiera, siendo una de sus limitantes, disponer en forma reducida de registros impresos sin considerar la totalidad de información guardada en medios magnéticos.

En este enfoque se determina la confiabilidad de las entradas y los registros obtenidos sin poder determinar la validéz de su procesamiento.

Sin embargo, se advierte que para efectuar el estudio del control interno se incluye el análisis y la comprensión de los métodos que se utilizan para procesar la información y si el PE forma parte del control interno y produce la información, el auditor debe realizar su estudio y evaluación, como resultado de su trabajo deberá documentar adecuadamente sus conclusiones sobre el efecto del PE en sus pruebas de auditoría.

Por lo tanto, el auditor está obligado a efectuar su revisión utilizando todos los elementos que le permitan asegurarse de que la información financiera es procesada adecuadamente.

Para realizar el estudio y evaluación del control interno se señala la definición de control interno y los principales objetivos del control interno en un ambiente de PE.

Control interno: " Comprende el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la razonabilidad y confiabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la administración."[7]

Objetivos básicos del control interno.

Controles internos contables.

a) La protección de los activos de la empresa.
b) La obtención de información financiera, veraz, confiable y oportuna.

Controles internos administrativos.

c) La promoción de la eficiencia en la operación del negocio.
d) Lograr que en la ejecución de las operaciones se cumplan las políticas establecidas por los administradores de la empresa.

Objetivos generales del control interno.

El control interno contable está diseñado en función de los objetivos de la organización para ofrecer seguridad razonable de que: las operaciones se realizan de acuerdo con las normas y políticas señalados por la administración.

Los objetivos de los controles contables internos son:

Objetivos generales de control interno aplicables a todos los sistemas y

objetivos de control interno aplicables a ciclos de transacciones.

Los objetivos de control aplicables a todos los sistemas se desarrollan a partir de los objetivos básicos de control interno,

[7] *I.M.C.P., Normas y Procedimientos de Auditoría.*

los objetivos de control de ciclos se desarrollan a partir de los objetivos generales de control de sistemas, para ser aplicadas a las distintas clases de transacciones agrupadas en un ciclo.

Los objetivos generales de control interno de sistemas son:

Objetivos de autorización.

Todas las operaciones deben realizarse de acuerdo con autorizaciones generales o específicas de la administración.

Objetivos de procesamiento y clasificación de transacciones.

Todas las operaciones deben registrarse para permitir la preparación de estados financieros de conformidad con principios de contabilidad generalmente aceptados o de cualquier otro criterio aplicable a dichos estados y para mantener en archivos apropiados datos relativos a los activos sujetos a custodia.

Objetivos de salvaguarda física.

El acceso a los activos sólo debe permitirse de acuerdo con autorizaciones de la administración, y

Objetivos de verificación y evaluación.

Los datos registrados a los activos sujetos a custodia deben compararse con los activos existentes a intervalos razonables y tomarse las medidas apropiadas respecto a las diferencias que existan. Asimismo, deben existir controles relativos a la verificación y evaluación periódica de los saldos que se informan en los estados financieros, ya que estos objetivos complementan en forma importante a los mencionados anteriormente.

Estos objetivos generales de control interno de sistemas son aplicables a todos los ciclos.

Ahora bien, de este planteamiento se determina que el Area de Informática puede interactuar en el control interno como herramienta de apoyo y tener un control interno del Area y del departamento de Informática, por lo tanto, se puede considerar como objetivos del control interno de informática:

- La protección adecuada de los activos de la empresa por medio del control para que se obtenga la información en forma veraz, oportuna y confiable.

- Mejorar la eficiencia de la operación mediante la informática.

- Y que en la ejecución de las operaciones de informática se cumplan las políticas establecidas por la administración.

La diferencia entre los objetivos de control interno desde el punto de vista contable-financiero, mientras estén enfocados a la evaluación de la empresa mediante la revisión contable financiera y de otras operaciones, los objetivos de control interno a informática están orientados a todos los sistemas en general, al equipo de cómputo, y al departamento de informática.

Para los objetivos de control interno, desde el punto de vista contable-financiero, es necesario que el auditor cuente con las herramientas adecuadas para apoyarse y con las técnicas que se han mencionado en el punto anterior "Auditoria con la computadora", se establezca una metodología para la revisión de los sistemas de aplicación de la empresa y además asegurarse de la integridad del procesamiento mediante controles adecuados.

O bien, crear una metodología que garantiza una revisión más extensa e independiente de los sistemas de informática que podrían ser:

- Selección de un sistema de información que se va a revisar.

- Obtención de la documentación de los archivos que incluye: nombre del archivo y descripción, nombre de los campos y descripción, (longitud, tipo), codificación empleada, etc.

- Trasladar el archivo de datos a una microcomputadora con una gran capacidad de almacenamiento.

- Llevar a cabo con un software de auditoría las verificaciones de auditoría que se mencionan anteriormente.

- Participación del auditor interno en el desarrollo de sistemas.

La participación de la auditoría interna en el desarrollo de sistemas permite asegurar que se tengan los controles de acuerdo con las políticas internas antes de iniciar la programación, en este diseño general y detallado de los sistemas, debe incluirse personal de auditoría que habrá de tener conocimientos de informática, pero no se requerirá de especialistas ya que sólo intervendrán en el diseño general del sistema, diseño de controles, sistemas de seguridad, respaldo y confidencialidad del sistema, sistemas de verificación, comprobación de lo señalado en el diseño general sea igual a lo obtenido en el momento de implantación, para autorizar la corrida en paralelo.

Sin embargo, no es tan fácil esta situación debido a la exigencia que crea el propio departamento de informática, el auditor que participe en este proceso debe contar con una mezcla de conocimientos que le permita tener una comprensión adecuada del trabajo que está realizando, estos incluyen un conocimiento del diseño conceptual de las aplicaciones, de la descripción y organización de los datos, de las etapas del proceso de datos, programación, lenguajes, y del ambiente en que operan, además de los conocimientos de las labores de auditoría.

Así como también el auditor debe participar en la planeación de los procedimientos de auditoría ya que revisando el requerimiento de informática, las ventajas que ofrece para el nuevo sistema, el auditor debe sugerir rutinas dentro de los programas que permitan accesar la información, por lo tanto el auditor debe tener la habilidad para supervisar y probar la integridad de los sistemas, para ello debe tener los conocimientos mencionados.

De la misma manera, el auditor debe efectuar una evaluación al área de informática en cuanto a la estructura del departamento, planes y objetivos, métodos y controles, forma de operación y facilidades humanas y técnicas.

Por consiguiente se observa que la capacidad profesional y entrenamiento técnico que el auditor ha tenido, le ha permitido hacer suya la labor de auditoría financiera, la cual la fue realizando hasta utilizar el computador, pero las necesidades de crecimiento y desarrollo en las empresas, ha exigido que esta área de informática sea evaluada en toda su extensión y es por este motivo que el auditor necesita además de su preparación, capacitación adicional como ya se ha indicado.

Con estas especificaciones de revisión necesarias para el control que requiere la información procesada se determina que el auditor que efectúe la auditoría en informática debe tener alto grado de conocimiento en informática y con mucha experiencia en el área.

Si no es así la puede efectuar un especialista en proceso de datos, un asesor o auditor apoyado de un especialista en proceso de datos, pero en este caso el auditor con capacidad profesional y entrenamiento técnico suficiente, dirigirá la auditoría.

Aquí se refiere a una auditoría en un ambiente de informática por lo que se concluye que la informática es una disciplina que está en constante desarrollo tecnológico y al mismo tiempo avanza en el desarrollo de paquetes, motivo por el cual para la realización de la auditoría en informática se necesita al especialista técnico que este familiarizado en éste aspecto con la experiencia suficiente, otro especialista con experiencia en

el diseño y análisis de sistemas para la participación del área de auditoría informática en el desarrollo de sistemas, el área de auditoría informática debe tener obviamente contadores con la experiencia en informática, licenciados en administración, con experiencia en contaduría y finanzas, familiarizados con el ambiente de sistemas informáticos, ambos con capacidad de análisis.

Personal que intervendrá

El personal que intervenga en la auditoría, debe estar debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de los recursos.

Se debe tener personal asignado por la empresa con el suficiente nivel para coordinar la auditoría y proporcionar la información requerida y además programe las entrevistas o reuniones, de esta forma se va iniciando la creación de un grupo multidisciplinario.

Para ir agregando más personal se debe tener personal asignado por los usuarios para los casos de requerir información o comprobación de algún proceso.

Para complementar el grupo, como colaboradores directos en la realización de la auditoría se debe tener personal con las siguientes características:

- Técnico en informática
- Conocimientos de administración, contaduría, finanzas
- Experiencia en el área informática
- Conocimientos y experiencia en psicología industrial
- Conocimientos de los sistemas más importantes

En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como redes, bases de datos, etc.

La auditoría puede ser solicitada por un tercero o el mismo departamento desarrollador de sistemas y puede ser en forma esporádica, externa, interna o permanente.

Se incorpora una estructura para el Departamento Interno de Auditoría Informática, independientemente de la forma en que se desarrolle la auditoría.

- Dirección General
- Dirección de Auditoría
- Gerente de auditoría informática
- Jefe de sistemas en desarrollo
- Jefe de sistemas automatizados y en operación

1.3.4. FUNCIONES DEL AUDITOR EN INFORMÁTICA

Partiendo de los objetivos generales de la Auditoría Informática que son:

- Disminuir los riesgos de las operaciones de la empresa relacionadas con el procesamiento de datos, tanto en el desarrollo y operación de sistemas como en las instalaciones de cómputo.

- Apoyar a las áreas de Auditoría y Contraloría en su incorporación paulatina hacia métodos automatizados de revisión.

- Participar en el proceso de desarrollo de sistemas, con objeto de vigilar la adecuada administración del proyecto y que los controles necesarios sean instrumentados.

- Supervisar las funciones del área de sistemas para evaluar la confiabilidad y seguridad de los sistemas de información en operación.

- Evaluar las medidas de seguridad implantadas en las áreas de procesamiento de datos, para proteger las instalaciones equipos y la información, contra siniestros. Se verán algunas de las evaluaciones del auditor en informática dividida por áreas funcionales de aplicación.

Evaluaciones Generales

1. Sistemas en desarrollo

- Planeación de proyectos
- Aprobación
- Estudio de factibilidad
- Análisis de costo-beneficio

2. Sistemas automatizados en operación

- Documento fuente
- Inicio de transacciones
- Seguridad de acceso al sistema
- Corrida de aplicaciones
- Emisión y distribución de información

3. Administración y seguridad de centros de procesamiento

- Calendarización y control de producción
- Controles de acceso y seguridad física
- Cintoteca, respaldos y software del sistema

- Procedimientos de respaldo y recuperación
- Planes de contingencia

4. Sistemas avanzados de cómputo

- Sistemas de base de datos
- Sistemas basados en procesamiento distribuido
- Redes de comunicación de datos
- Sistemas descentralizados basados en minis y microcomputadores

5. Salvaguarda de los activos de cómputo y mantenimiento

- Cobertura de seguros e información de activos actualizada (íntegra, precios reales, moneda, etc.)
- Programas de mantenimiento preventivo, detectivos y correctivos

6. Aspectos generales de sistemas

- Cumplimiento y actualización del plan de sistemas
- Uso y aprovechamiento de recursos informáticos
- Admnistración del área

7. Apoyo técnico a las áreas de auditoría en aspectos de cómputo

- Uso y aprovechamiento de recursos informáticos centralizados
- Automatización de los procedimientos de auditoría
- Automatización de las funciones administrativas de auditoría
- Auditoría con y a través del computador

Funciones.

Planeación de la auditoría.

Se debe efectuar una planeación de la auditoría informática en base a sus objetivos, se requiere obtener información general sobre la empresa y sobre la función informática a evaluar, se debe efectuar una investigación preliminar, y algunas entrevistas previas y efectuar un programa de actividades incluyendo, personal, tiempo, costo y documentos auxiliares a solicitar durante el desarrollo de la auditoría.

Ejecución del trabajo.

Elaborada la planeación de la auditoría, se procede a efectuar la revisión sistematizada del área através de la observación y entrevistas en cuanto a:

Estructura orgánica.

Jerarquías. (definición de la autoridad lineal, funcional y de asesoría)
Estructura orgánica.
Funciones
Objetivos
Revisión en cuanto a la situación de los recursos humanos.
Efectuar entrevistas con el personal de PE
Jefatura
Análisis
Programadores
Operadores
Capturistas
Personal administrativo

Debe conocer la situación presupuestal y financiera

Presupuesto
Recursos financieros
Recursos materiales
Mobiliario y equipo

Debe efectuar entrevistas o cuestionarios para hacer un levantamiento de censo de recursos humanos y análisis de situación en cuanto a:

Número de personas y distribución por áreas
Denominación de puestos
Salario
Capacitación
Conocimientos
Escolaridad
Experiencia Profesional
Antigüedad
Historial de trabajo
Salario y conformación
Movimientos salariales
Índice de rotación de personal
Programa de capacitación (vigente y capacitación dada en el último año)

Finalmente se debe revisar el grado de cumplimiento de los documentos administrativos.

Normas y políticas
Planes de trabajo
Controles
Estándares
Procedimientos

1.3.5. TIPOS DE AUDITORIA INFORMÁTICA.

A. Apoyo (controles gerenciales)

B. Específica
   Hardware (instalaciones, equipo y seguridad física)
   Software (selección sistemas, sistemas y programación)
   Personal (administración del personal)
   Administración (equipo, instalación, personal
   comité de revisiones y efectivo control org.)

C. Situación del inventario (asignación de los equipos a las áreas de trabajo)

D. Integral (todos los anteriores).

2. CONTROL INTERNO Y CONTROLES EN LOS SISTEMAS DE INFORMACION

2.1 DEFINICIÓN DE CONTROL INTERNO

Para comenzar daremos algunas definiciones, según la definición de la Comisión de Normas y Procedimientos de Auditoría, es la siguiente: " El control interno comprende el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la razonabilidad y confiabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la administración. "[8]

Sin embargo podemos reducir ésta definición tomando la siguiente del Ing. J. M. Gutiérrez: " El plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para la consecución de sus objetivos. "[9].

Dichos objetivos se han definido como controles internos contables y controles internos administrativos.

Los controles internos contables comprenden el plan de organización y los procedimientos y registros que se refieren a la protección de activos y a la confiabilidad de los registros financieros, por lo que los objetivos contables son:

a) Protección de los activos de la empresa.

b) Obtención de información financiera veraz, confiable y oportuna.

---

[8] *I.M.C.P. Boletín E-02 Control Interno.*
[9] Gutiérrez J. José M. APUNTES.

Los controles internos administrativos se refieren a la información operativa de tipo estadístico, registro de acceso a ciertas instalaciones de la empresa. Por lo tanto los objetivos administrativos son:

a) Promoción de eficiencia en la operación del negocio

b) La ejecución de las operaciones se adhiera a las políticas establecidas por la administración de la empresa.

También incluimos los objetivos generales del control interno que son aplicables a todos los sistemas, por lo tanto, La Comisión de Normas y Procedimientos de Auditoría nos dice: " Cuando hablamos de los objetivos de los controles contables internos podemos identificar dos niveles:

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

b) Objetivos de control interno aplicables a ciclos de transacciones.

Los objetivos generales de control aplicables a todos los sistemas se desarrollan a partir de los objetivos básicos de control interno enumerados anteriormente, siendo más específicos para facilitar su aplicación.

Los objetivos de control de ciclos se desarrollan a partir de los objetivos generales de control de sistemas, para que se apliquen a las diferentes clases de transacciones agrupadas en un ciclo."[10]

Los objetivos generales de control interno aplicables a todos los sistemas se describen a continuación apoyados del boletín E-02.

Objetivos de autorización.

- Todas las operaciones deben realizarse de acuerdo con autorizaciones generales o especificaciones de la administración.

- Las autorizaciones deben estar de acuerdo con criterios establecidos por el nivel apropiado de la administración.

- Las transacciones deben ser válidas para conocerse y ser sometidas oportunamente a su aceptación. Todas aquellas que reúnan los requisitos establecidos por la administración deben reconocerse como tales y procesarse a tiempo.

[10]I.M.C.P. BOLETIN E02. CONTROL INTERNO.

- Los resultados del procesamiento de transacciones deben comunicarse oportunamente y estar respaldados por archivos adecuados.

Objetivos del procesamiento y clasificación de transacciones.

- Todas las operaciones deben registrarse para permitir la preparaciónón de estados financieros en conformidad con los principios de contabilidad generalmente aceptados o por cualquier otro criterio aplicable a los estados y para mantener en archivos apropiados los datos relativos a los activos sujetos a custodia.

- Las transacciones deben clasificarse en forma tal que permitan la preparación de estados financieros en conformidad con los principios de contabilidad generalmente aceptados y el criterio de la administración.

- Las transacciones deben quedar registradas en el mismo periodo contable, cuidando específicamente que se registren aquellas que afectan más de un ciclo.

Objetivo de salvaguarda física.

- El acceso a los activos sólo debe permitirse de acuerdo con autorizaciones de la administración.

Objetivo de verificación y evaluación

- Los datos registrados relativos a los activos sujetos a custodia deben compararse con los activos existentes a intervalos razonables y tomar las medidas apropiadas respecto a las diferencias que existan.

- Deben existir controles relativos a la verificación y evaluación periódica de los saldos que se incluyen en los estados financieros.

Estos objetivos generales del control interno de sistemas son aplicables a todos los ciclos.

El área de informática puede interactuar de dos maneras en el control interno.

La primera se utiliza como una herramienta por medio de paquetes de auditoría y la segunda se lleva a cabo el control interno de informática los cuales son:

- Proteger adecuadamente los activos de la organización por medio del control para que se obtenga la información en forma veraz, oportuna y confiable.

- Se mejore la eficiencia de la operación de la organización mediante la informática.

- Se cumplan las políticaas establecidas por la administración.

La diferencia que el Lic. J. A. Echenique nos marca entre los objetivos de control interno contable-financiero es que mientras éstos están enfocados a la evaluación de una organización mediante la revisión contable-financiera y de otras operaciones, los objetivos del control interno a informática están orientados a todos los sistemas en general, al equipo de cómputo y al departamento de informática, para lo cual se requieren conocimientos de contabilidad, finanzas, recursos humanos, administración, etc., y un conocimiento profundo y experiencia en informática.

2.2 ELEMENTOS Y SUBELEMENTOS DEL CONTROL INTERNO EN LA GESTIÓN INFORMÁTICA.

Los elementos del control interno, se constituyen de la siguiente manera:

a) Organización.

Este primer elemento del control interno, persigue dar cohesión a los objetivos y propósitos organizacionales, con los objetivos y funciones informáticas así como los recursos necesarios para el logro de las metas y el cabal cumplimiento de propósitos encomendados.

a.1) Dirección: Este elemento representa la función de dirigir todos los recursos de una organización hacia el logro de los objetivos organizacionales. La gestión informática se convierte en una pieza fundamental y estratégica de la misma empresa.

Influencia en el PED: La dirección de los recursos de una empresa hacia sus objetivos a corto, mediano y largo plazo involucra recursos computacionales (equipo, tecnología y recursos humanos).

a.2) Coordinación: Este elemento pretende que se adopten las obligaciones y necesidades de las partes integrantes de la empresa a un todo homogéneo y armónico; que prevea los conflictos propios de invasión de funciones o interpretaciones contrarias a las asignaciones de autoridad.

Por un lado se requiere saber hacia donde se dirigen las actividades y los recursos y por otro lograr la capacidad para conjuntarlos armónicamente en función de los propósitos

establecidos.

Influencia en el PED: La coordinación de los subsistemas de una organización puede verse afectada por la incorporación del PED. Para ello es necesario identificar la actividad e integrar adecuadamente el equipo necesario y considerar los objetivos a corto y largo plazo de la empresa y de informática para incorporar recursos apropiados a su desarrollo táctico y estratégico.

a.3) División de funciones: Este elemento involucra la división de funciones entre las áreas o personal de la empresa, no únicamente para evitar duplicidad de funciones, sino también para segregar funciones incompatibles, es decir, que se definan claramente la independencia de las funciones.

Influencia del PED: El PED normalmente altera los lineamientos ortodoxos de división de labores y origina nuevas actividades que deben adaptarse a una segregación de funciones adecuada.

En el ambiente de informática los recursos de equipo y registros requieren ser operados por funciones que tengan distinción entre el acceso y su disposición para no interferir en la calidad y debida salvaguarda de los mismos.

a.4) Asignación de responsabilidades: Este elemento asegura que se defina quien es responsable de cada una de las funciones de la organización, asegurando de alguna forma que se adopte el compromiso de lograr los objetivos establecidos para dichas funciones.

Influencia del PED: Los conceptos de autoridad y responsabilidad adquieren nuevas dimensiones en un ambiente de PED. Por lo que es necesario identificar y documentar las principales funciones su importancia es no generar redundancia tanto a la función informática como en los usuarios.

b) Procedimientos.

Este elemento del control interno se deriva de la organización, tiende a formalizar y regular operativamente, es reflejo tanto de lineamientos directivos, como de estructuras de coordinación y definición de labores.

b.1) Planeación y sistematización: Debe existir una planeación adecuada de actividades tanto a corto, mediano como largo plazo, de igual forma se debe contar con sistemas, manuales e instructivos que permitan desarrollar las funciones de la organización en una forma metodológica y estandarizada.

Influencia del PED: El PED requiere nuevos manuales de estándares y procedimientos y un enfoque diferente sobre los sistemas de información.

b.2) Registros y formatos: Deben existir medios para registrar la información relativa a las operaciones que realiza la empresa, estos medios son normalmente el uso de formatos pre-impresos y/o predefinidos que faciliten el registro y consulta de información.

Influencia del PED: El registro de operaciones puede llegar a ser completamente en medios magnéticos lo cual requiere de formatos adecuados para la codificación de datos y para la conservación de los mismos.

b.3) Informes: La administración de la compañía debe contar a todos sus niveles con informes que le permitan conocer la situación de la empresa y de las operaciones que ésta realiza.

Influencia del PED: El PED propicia el riesgo de emitir gran cantidad de informes sin tomar en cuenta su calidad o utilidad práctica. No cuenta con sistemas informativos propios, queda en las áreas de Contraloría y/o auditoría para contribuir bajo estructuras preventivas el control de esta actividad en el desarrollo de labores, nivel de servicio, acceso a la información y programas e impacto económico de los servicios informáticos.

c) Personal.

Las organizaciones se están haciéndo más dependientes de la gestión informática, lo que obliga a fortalecer el elemento humano en función a sus niveles de responsabilidad y de la sensibilidad de las labores asignadas.

c.1) Entrenamiento: El personal de una empresa debe contar con un entrenamiento adecuado al tipo de actividad que desarrolla.

Influencia del PED: La tecnología de computación tiene un desarrollo acelerado por lo que los conocimientos adquiridos se vuelven obsoletos con más rapidez que en ninguna otra disciplina.

c.2) Eficiencia: El personal que labore en una organización debe observar un desempeño eficiente, es decir, debe optimar la utilización de sus recursos.

Influencia del PED: La eficiencia de las actividades adquiere mayor importancia debido a lo costoso de los recursos computacionales.

c.3) Moralidad: Un factor indispensable en el personal de una organización es la moralidad que rija su conducta. Es obvio que la moralidad del personal es una de las columnas sobre las que descansa la estructura del control interno.

Influencia del PED: La concentración de información en un solo departamento de la empresa y las capacidades del personal del PED para accesarla, proporcionan a la moralidad un valor considerable dentro de los elementos del control interno.

c.4) Retribución: Un elemento importante para el personal es el percibir una adecuada retribución por el trabajo que desempeña, esta retribución no necesariamente debe ser económica. Esto hará que se preste mejor a realizar los propósitos de la empresa con entusiasmo y eficiencia.

Influencia del PED: Generalmente el personal de informática a niveles operativos tiene una remuneración superior a otras áreas de la empresa, debido a que vuelven " grupos de poder " por controlar la información de la compañía y crear dependencia.

d) Supervisión.

Este último elemento de control interno enmarca un enfoque integral, representa un agente de control de las organizaciones el cual debe verificar que las actividades realizadas se apeguen a los lineamientos y políticas preestablecidas en la empresa, la supervisión se ejerce en diferentes niveles, por diferentes funcionarios y empleados y en formas directa e indirecta.

Influencia del PED: La supervisión de cualquier actividad requiere de conocimientos y experiencia sobre la misma.

2.3 TIPOS DE CONTROL

El propósito de un control es asegurarse de que un sistema está funcionando en debida forma. Los buenos controles presuponen estándares cuidadosamente desarrollados, que ayudan a todas las áreas de la organización a decidir cuando una operación es inaceptable, satisfactoria u óptima.

Clasificación con base a su objetivo o función.

- Preventivos: Son los procedimientos de control que pretenden prevenir o evitar la ocurrencia de errores. Este tipo de control normalmente se aplica en forma individual a las transacciones y consiste en procedimientos tales como: formatos preimpresos, políticas, estándares, programas de capacitación etc.

- Detectivos: Estos controles se utilizan para detectar la ocurrencia de un error, son controles que reaccionan cuando un error ya ocurrió. Normalmente se aplican a grupos de transacciones (aunque no necesariamente) y al final de algún proceso. P. E. cifras, control, passwords, conciliación de cifras, etc.

- Correctivos: Estos procedimientos tiene un carácter correctivo, pues son los que se utilizan una vez identificado un error (mediante controles detectivos) para corregirlo y realimentarlo al flujo de la operación. Estos controles consisten normalmente en actividades definidas en manuales de procedimientos.

Clasificación con base a su esencia.

- Controles funcionales: Son aquellos procedimientos de control que forman parte de un proceso o actividad, su aplicación es parte integrante de dicho proceso, por lo que su exclusión puede afectar el flujo de alguna operación o sus resultados. P. E. La verificación de las existencias en inventario antes de surtir un pedido.

- Controles intrínsecos: Son aquellos que no forman parte del proceso, sino que su función es puramente de control. Su ausencia no afecta el proceso rutinario, sin embargo puede ocasionar otro tipo de problemas. P. E. Un procedimiento de conciliación de cifras control.

2.4 CLASIFICACIÓN DEL CONTROL INTERNO EN SISTEMAS.

El área de procesamiento electrónico de datos se encarga de captar, procesar y producir información que le permite a la organización tomar decisiones adecuadas, por lo tanto, es de suma importancia que los controles establecidos en ésta deban enfocarse a la creación, a través de políticas y procedimientos adecuados, de un sistema que asegure que toda la información que deba ser procesada, se procese en forma correcta y oportuna, y que dicho proceso se obtenga la información esperada, por lo que surgen dos tipos de controles para el área de Procesamiento Electrónico de Datos:

A) Controles generales: Se refiere al estudio y evaluación de todas las actividades generales de PED y a las funciones de quienes intervienen en el desarrollo de sistemas, esto es, el medio ambiente en donde se desarrollan los sistemas tales como:

1. Controles de Pre-instalación
2. Controles de Organización
3. Controles de desarrollo
4. Controles de operación
5. Controles de procesamiento

6. Controles de documentación

B) Controles de aplicación: Se refieren al estudio y evaluación de los procedimientos de control establecidos para cada aplicación específica en la operación del computador que incluye la entrada, proceso y salida de datos, tales como:

1. Procedimientos manuales
2. Procedimientos de control de datos
3. Procedimientos de entrada de datos
4. Procedimientos de proceso de datos
5. Procedimientos de salida de información
6. Procedimientos de almacenamiento de información
7. Procedimientos de distribución de información.
8. Documentación.

A) CONTROLES GENERALES

2.4.1 CONTROL PRE-INSTALACIÓN.

Se refiere al estudio de viabilidad y selección de equipo que debe efectuarse previo a la adquisición de un equipo de cómputo, así como el acondicionamiento físico y medidas de seguridad en el área donde se localiza el equipo y a la capacitación de personal y adquisición o desarrollo de sistemas.

Los tres principales objetivos que deben cubrir los controles de pre-instalación son:

a) Asegurarse de que el computador se ordenará siempre y cuando pueda preverse que producirá mayores beneficios que cualesquiera de las otras alternativas de automatización.

b) Asegurar la selección de servicios adecuados.

c) Asegurarse de que se elabore un plan de pre-instalación contra el cual verificar los resultados y el avance.

Estándares mínimos de control.

1) Debe haber un método que asegure que los costos, economías, beneficios y métodos de procesamiento resultantes de la introducción del computador podrán determinarse aproximadamente, antes de que se tome la decisión de adquirir el computador.

- Debe formarse un Comité gerencial con responsabilidad para iniciar, guiar y revisar los resultados de la investigación preliminar.

- El Comité gerencial deberá elaborar la Guía de referencia para el estudio preliminar.

- Deberá llevarse a cabo una investigación preliminar y prepararse un informe de la investigación de acuerdo con la Guía de referencia.

- Se deberá formar un Comité de dirección del proyecto de computación, el cual iniciará, dirigirá y revisará la elaboración del estudio de factibilidad.

- Deberá elaborarse un Estudio de factibilidad y prepararse un informe de acuerdo a las Guías de referencia.

2) Debe establecerse e identificarse un criterio adecuado de selección del equipo y hacerlo del conocimiento de los posibles proveedores.

- Se deberá elaborar por escrito la lista de los criterios adecuados para la selección del equipo y hacerla del conocimiento de cada proveedor en potencia.

3) Un criterio selectivo se debe aplicar en la evaluación de las propuestas de los proveedores.

- El criterio de seleccción deberá establecerse en forma de un cuadro en el que se anotará la evaluación de las propuestas de los proveedores.

- Programas-paquete de simulación pueden utilizarse en la evaluación de las propuestas de los fabricantes.

- Los convenios contractuales deben ser revisados cuidadosamente en forma previa a la selección final del equipo y firma del contrato.

4) Deben identificarse y definir las labores o actividades de pre- instalación.

- Deberá prepararse un listado de todas las actividades o labores mostrando su interdependencia.

5) Todas las labores deben incorporarse a un programa de actividades.

- Las labores o actividades deben presentarse de manera que muestre su interdependencia y la relación de tiempo.

2.4.2 CONTROLES DE ORGANIZACIÓN.

Comprende la correcta estructura organizacional del departamento, principalmente la adecuada segregación de labores, la definición de políticas, funciones y responsabilidades, así

como la asignación de personal competente.

Los dos principales objetivos que deben cubrir los objetivos de controles de organización son:

a) Proporcionar un control efectivo de organización sobre la concentración de funciones en el departamento de procesamiento de datos.

b) Asegurarse que la gerencia ejerza un control efectivo acerca del despliegue de elementos en el computador.

Estándares mínimos de control.

1) El departamento de procesamiento de datos deberá independizarse de funciones incompatibles dentro de la organización.

- Deberá haber una separación de las funciones de: iniciación y autorización de transacciones, registro de transacciones y custodia de activos.

2) Deberá haber una segregación de labores en el departamento de PED.

- Las funciones de diseño de sistemas y programación deberán permanecer separadas de la operación del computador.

- Establecer un grupo de control de datos, independiente de las otras funciones de operación.

3) Se deberá mantener una separación normal de labores para propósitos de control en el departamento de origen y el departamento de usuario.

4) Se deberá contar con políticas de personal que propicien los controles en las funciones de PED.

- Adecuadas medidas de seguridad (cambio a códigos de conexión y códigos de identificación) después que los empleados han terminado sus contratos.

- Devolución de tarjetas de identificación, llaves, documentación y demás material de la compañía, de los empleados que han terminado sus contratos de trabajo.

- Rotación de tareas.

2.4.3 CONTROLES DE DESARROLLO.

Estos controles son muy importantes ya que se establecen desde usuarios hasta la implantación de un sistema, es decir, estos controles se aplican a través del proceso de desarrollo de sistemas, desde el análisis de las necesidades del usuario hasta la implantación de una aplicación.

Por lo tanto, los controles estarán enfocados básicamente al establecimiento de una metodología idónea para el análisis, diseño, implantación y mantenimiento de los sistemas de información.

Los grupos que intervienen para el desarrollo y mantenimiento de sistemas son:

a) Alta gerencia (usuario)
b) Departamentos usuarios
c) Diseñadores de sistemas
d) Programadores
e) Auditoría interna (para verificar la implantación de controles)

Los objetivos de los controles de desarrollo y mantenimiento de sistemas pueden ser para:

a) Asegurar que una aplicación sea convertida al computador, solamente si va a producir mayores beneficios que cualquier otra alternativa.

b) Asegurar el desarrollo de sistemas y programas efectivos.

c) Asegurar que los sistemas y programas sean mantenidos con efectividad.

d) Los sistemas sean modificados única y exclusivamente cuando sea justificado y bajo los mismos controles que se aplicaron en sus desarrollo.

Estándares mínimos de control.

1) Deberá haber una metodología bien definida para garantizar que los costos, ahorros, beneficios y métodos resultantes de la introducción del procesamiento en computador, puedan ser determinados aproximadamente, antes de que se tome la decisión de adquirir un computador o de agregar al computador una aplicación.

- Se deberá efectuar un estudio de factibilidad efectivo.

- La alta gerencia deberá aprobar las conclusiones de los diferentes grupos de estudio.

2) Se debe hacer una planeación a largo plazo como guía para el diseño de los sistemas subsecuentes.

3) Deberá haber una participación activa de representantes de departamentos usuarios, incluyendo el departamento de contabilidad.

La función del especialista en sistemas comprenderá:

a) Elaborar gráficas de flujo detalladas, formato de registro, de archivos y de documentos de entrada y salida.

b) Elaborar especificaciones de control.

c) Participar en el diseño de los procedimientos que se seguirán en el departamento usuario para el nuevo sistema fuera del centro de cómputo, y los procedimientos de conversión necesarios.

d) Elaborar las instrucciones de operación.

4) Deberá haber una separación de labores y asignación de responsabilidades proporcionales con las funciónes no compatibles y la experiencia y habilidades que se requiere.

- Se debe separar las funciones de programación y operación.

- El departamento de PED, no debe tener control sobre los activos o sobre el origen de las transacciones, el control lo deben tener los usuarios responsables de la operación.

5) Se deberán establecer estándares para el diseño de sistemas y de técnicas y procedimientos de programación.

- Deberán establecerse, documentarse y ponerse en práctica, estándares de diseño de sistemas.

a) Para la requisición, coordinación y aceptación del usuario.
b) Para el análisis y diseño de sistemas
c) Para la prueba de sistemas
d) Para la implantación de sistemas
e) Para modificaciones a sistemas en producción.
f) Documentación
g) Para la programación
h) Para la nomenclatura de programas archivos, bibliotecas y listados.
i) Para la conversión e implantación de sistemas.

6) Cada fase importante del desarrollo, debe ser autorizada y aprobada.

- Cada sistema debe revisarse y aprobarse por la alta gerencia y departamentos usuarios en forma previa a la iniciación del diseño de sistemas.

- Se deberá establecer una metodología de revisión del avance realizado, para compararlo con el avance previsto.

- Antes de la operación del nuevo sistema, se debe obtener la aprobación final.

7) Los sistemas y los programas deberán ser aprobados exhaustivamente para asegurar su consistencia con las especificaciones originales.

- Deberá existir cooperación entre el usuario y el departamento de desarrollo de sistemas para la prueba de los sistemas.

- Las pruebas finales, deberán comprender todas las fases del sistema, incluyendo las de uso del computador y las del procesamiento manual.

- Se debe ejercer control acerca de la conversión de los archivos maestros, para prevenir modificaciones no autorizadas a los mismos y para garantizar resultados confiables y completos.

8) Las modificaciones a los sistemas y programas deberán estar sujetas a los mismos controles que los sistemas nuevos.

- Debe obtenerse autorización previa al inicio de la modificación.

- Los operadores no deben estar autorizados para hacer modificaciones (no importando su trascendencia)

- Deben controlarse las pruebas y la aprobación final de las modificaciones.

- La sección de operaciones, solo adoptará modificaciones si están debidamente aprobados.

9) Se debe mantener un control adecuado en la sección de operaciones para evitar modificaciones no autorizadas.

10) Si son programas realizados por proveedores externos es necesario contar con procedimientos de control sobre la adquisición de los programas que requieren la revisión de documentación y de los controles de procedimiento.

2.4.4 CONTROLES DE OPERACIÓN.

Estos controles están directamente relacionados con las operaciones de procesamiento de datos y en consecuencia ayudan a asegurar que las transacciones son manejadas apropiadamente y que los datos sean convertidos de una forma precisa y segura en información.

Los objetivos que persiguen estos controles pueden ser entre otros:

a) Prevenir o detectar errores accidentales que ocurran en el departamento de PED durante el proceso.

b) Prevenir o detectar la manipulación fraudulenta de los datos en su procesamiento por el departamento de PED y prevenir el mal uso de información confidencial.

c) Proporcionar seguridad en contra de la destrucción accidental de los registros y asegurar una operación contínua.

Estándares mínimos de control.

1) Deberá existir un método bien definido que asegure que los datos estén completos y exactos y estèn autorizados al recibirlos para su procesamiento.

- Deberá establecerse un grupo de control que reciba todos los datos para su procesamiento, y asuma la responsabilidad de ver que todos los errores detectados durante el procesamiento, serán corregidos y asegurar que toda la información de salida (output) se distribuya adecuadamente.

- La edición de los programas del computador deberá usarse en la extensión que sea posible, para verificar la totalidad, exactitud y autorización adecuadas de los datos y para complementar las funciones del grupo de control.

2) Deberán usarse procedimientos estandar para todas las operaciones y hacer una revisión con el fin de asegurar que cumplan con estos procedimientos.

- Deberán proporcionar manuales de sistemas y procedimientos para todas las funciones en las operaciones del computador.

a) Control de datos
b) Conversión de datos
c) Operaciones del computador
d) Almacenamiento de archivos

- El método utilizado por el computador para el control de sus propias operaciones deberá ser evaluado desde el punto de vista de los requisitos generales de control.

- Los procedimientos seguidos deben ser revisados por el supervisor de operaciones.

3) Deberá existir un método bien definido que asegure el correcto montaje de los archivos, la correcta colocación de interruptores y la localización adecuada de archivos de salida.

- Los archivos del computador deben llevar etiquetas internas y externas.

- El sistema operativo o los programas del computador deberán utilizarse al máximo posible para comprobar procedimientos de inicialización de archivos y de máquina.

4) Deberá existir un procedimiento previamente definido que asegure la oportuna detección de errores y fallas de hardware.

- Predeterminar y verificar periódicamente durante el procesamiento, los totales de los datos de entrada, de los archivos maestros y de salida.

- El computador deberá emplearse para la edición de los errores.

- Deberá haber un método debidamente definido para asegurar que el equipo esté trabajando adecuadamente.

5) El departamento de PED deberá ser independiente de los departamentos de origen y departamentos usuarios, dentro de la organización.

- Deberán estar separadas las funciones de programación y operación.

- Es deseable que los conocimientos de programación del operador sean limitados.

- Deberán revisarse las bitácoras de utilización de la máquina.

6) Deberán haber procedimientos estandar para prevenir o detectar errores accidentales, causados por error de operación o mal funcionamiento de la máquina o programa.

7) Deberá haber un procedimiento bien definido para reconstruir los archivos después de errores leves de procesamiento o destrucción de los registros.

- Se deben elaborar instrucciones explícitas de operación para casos de condiciones de error y de interrupción del procesamiento.

- Se deberán tener archivos de respaldo.

- Se deberán incluir procedimientos de verificación y de reinicio en cada programa con tiempo de procesamiento, mayor a treinta minutos.

8) Deberá haber una salvaguarda física de los archivos.

- Deberá existir un control del medio ambiente, contra los excesos de humedad, temperatura u otras condiciones atmosféricas.

- El cuarto del computador deberá estar protegido contra el fuego.

- Se deberán utilizar elementos de almacenamiento para archivos y programas fuera de la instalación.

9) Deberá existir un método bien definido que garantice la continuidad de las operaciones después de una destrucción importante de los archivos o de una falla mayor de equipo.

- Se deberán documentar los procedimientos que se requieran en condiciones de emergencia.

- Se deberá tener una póliza de seguros adecuada.

2.4.5 CONTROLES DE PROCESAMIENTO.

El procesamiento de datos deberá producir información confiable, completa y válida en forma oportuna, incluye procedimientos tanto en los departamentos de origen y usuario, como en el departamento de PED, los cuales ocurren en diferente orden cronológico e involucran personal diferente, dependiendo de la aplicación en particular.

Para que los controles de procesamiento operen con efectividad deberá existir un medio ambiente apropiado en los términos de la estructura organizacional, de los métodos para el desarrollo y mantenimiento de los sistemas y programas, y los procedimiento dentro de la instalación del computador.

Los principales objetivos de control de procesamiento son los siguientes:

a) Asegurar que la totalidad de los datos sean procesados por el computador.

b) Asegurar la exactitud de los datos procesados por el computador.

c) Asegurar que todos los datos procesados por el computador esten debidamente autorizados.

d) Asegurar que las pistas para la gerencia sean adecuadas.

Estándares mínimos de control.

1) Deberá haber un procedimiento bien definido que asegure que inicialmente son registrados e identificados la totalidad de los datos.

- Cada transacción deberá ser inicialmente registrada en una forma especialmente diseñada al efecto, la cual deberá llevar un código de identificación y llenarse de manera que se puedan hacer referencias subsecuentes a la misma.

- Donde sea posible el computador deberá ser programado para anticipar cada transacción y detectar fallas o extravíos en la alimentación de los datos.

- Los empleados encargados de la preparación de los datos de entrada o que tengan acceso a documentos de origen en blanco, no deberán tener acceso ni ser responsables acerca de los activos que estén relacionados con dichos documentos de origen, los programas del computador o el computador en sí.

2) Se deberá establecer el control cerca del origen de la transacción.

- Los datos de entrada deberán ser lotificados cerca del punto de preparación y establecerse totales de control de lotes, se deberán utilizar formas de encabezado del lote que contenga un código de identificación y registro del total de control del lote.

3) Los datos de salida deberán ser conciliados con los de entrada.

- Los totales de control de salida deberán conciliarse con los totales de control de entrada por el grupo de control.

- Como una alternativa, los totales de control de la salida deberán conciliarse con el computador contra los totales de control de entrada.

- Los datos de salida deberán ser listados para la verificación visual contra los documentos de entrada.

4) Deberá existir un método bien definido que asegure que las correcciones de todos los errores identificados, sean realimentados al sistema.

- Todos los datos de rechazo deberán ser registrados por el grupo de control en un listado de errores y anotarse en el mismo listado las correcciones al ser realimentadas, las operaciones aisladas, se investigarán.

- Se debe establecer un sistema bien definido para la corrección de errores y la realimentación de correcciones como una entrada de datos, y se deberán asignar responsabilidades acerca del comportamiento de esta función.

5) El horario de entrega de los datos de entrada y distribución de los datos de salida, deberán coordinarse adecuadamente en el procesamiento.

- Se deben revisar las conciliaciones de las cifras de control en las fechas de cierre de las operaciones, para asegurar que toda la información de entrada esté incluida en los datos procesados.

- Es recomendable que el grupo de control elabore una cédula de control de los datos, y comprobar los controles a intervalos lo suficientemente frecuentes con objeto de proporcionar el medio más eficiente de corrección de errores y reconstrucción de los archivos.

6) Deberán existir procedimientos para prevenir errores en la preparación de los datos de entrada o datos fuente, y para detectar y corregir cualquier error significativo que pudiera presentarse.

7) Deberán haber procedimientos que garanticen que únicamente se utilicen los archivos correctos.

8) Deberán aplicarse procedimientos para asegurar que los cálculos del programa se realicen en forma correcta.

9) Deberá existir un sistema de control sobre la operación física del sistema del computador.

- Deberán especificarse procedimientos escritos en manuales que indiquen las normas sobre la preparación de los documentos de orígen de los datos.

- En ausencia de otros controles, los códigos de identificación deberán incluir la técnica de verificación automática del dígito de control, para identificar los errores de codificación.

- Cuando sea adecuado editar o examinar la exactitud de los datos de entrada, se deberá utilizar la edición manual.

10) Asegurar que solo se procesen datos autorizados, los documentos de entrada deberán mostrar evidencia de autorización y ser revisados respecto a la misma, por el grupo de control.

- En un sistema de procesamiento en lotes, deberán establecerse procedimientos operativos para la autorización de entradas y para el examen posterior de las mismas sobre lo adecuado de estas autorizaciones.

- Hasta donde sea práctico, se deberán utilizar las rutinas del computador para la autorización de entradas y el examen subsecuente de la adecuada autorización.

11) Deberá existir un método bien definido para identificar y localizar los componentes de los registros del archivo y los documentos de entrada y salida involucrados en el proceso de una transacción o en la acumulación de un total.

- Cada documento y registro en el archivo magnético, deberá tener una identificación única.

- Cada documento y registro en el archivo magnético, deberá estar archivado en una secuencia planeada par facilitar su accesibilidad.

- Los métodos de rastreo de datos hacia el origen o hacia adelante deberán ser una parte integral del desarrollo de sistemas.

Las pistas de la gerencia y los procedimientos de referencia cruzada, deben incorporarse en el sistema, por el analista de sistemas, a fin de:

a) Determinar el contenido de los registros de detalle que integran un total o una cantidad sumaria en cualquier documento de salida.

b) Determinar el contenido de los registros de entrada a detalle y los registros del archivo maestro involucrados en la producción de cualquier resultado del proceso.

c) Asegurar la localización física de todos los documentos de entrada y salida procesados.

2.4.6 DOCUMENTACIÓN.

Necesidad de que todos los programas, la operación y los procedimientos relativos estén adecuadamente documentados y

actualizados. Es conveniente que se tenga copia-respaldo de esta documentación fuera de las instalaciones.

Los objetivos mínimos de documentación son:

a) Asegurar la existencia de la documentación que sea controlada y asegurada.

b) Asegurar que todos los sistemas son documentados adecuadamente.

c) Asegurar que todos los programas sean documentados adecuadamente.

d) Asegurar que las instrucciones al personal de PED y del usuario sean documentados adecuadamente.

Estándares mínimos de control.

1) Deberá existir un método bien definido para asegurar de toda la documentación: sistemas y documentos, se preparen de acuerdo a estándares previamente establecidos.

- Para ejemplificar de una manera más objetiva aquellas tares y/o funciones que deberán ser documentadas, presentamos en orden operativo los procedimientos de elaboración de cualquier sistema:

a) Definición del problema
b) Diseño del sistema
c) Programación
d) Procedimientos de operación
e) Procedimientos de biblioteca
f) Procedimientos de captación
g) Procedimientos de control
h) Procedimientos del usuario

2) Contar con copias de la documentación fuera de las instalaciones del centro de cómputo, así como la historia de los cambios efectuados.

B) CONTROLES DE APLICACIÓN.

2.4.7 CONTROLES DE ENTRADA.

Asegurar que toda la información que vaya a ser procesada por el computador esté completa y correcta y que existan controles adecuados para el manejo de información rechazada.

Todos los datos deben entrar al sistema una sola vez, la validación de la captura debe ser completa, con apoyo de los reportes de control.

Los errores deben ser indicados por el computador.

Se deben establecer los procedimientos de manejo de errores para garantizar que todos los errores posibles sean detectados y corregidos.

Es recomendable crear un dígito verificador en los datos de entrada, por captura se cometen errores.

Controles batch.

El sistema puede producir una serie de reportes sumarios con el total de información aceptada y rechazada, los cuales pueden contener el número de documentos procesados así como los totales de control, o bien, si los totales de control no son iguales a los que procesó el sistema, también pueden reportar las diferencias.

Reportes de control.

Para validar la corrección de los procesos realizados por el computador, es necesaria la verificación y conciliación de información a través de reportes de control.

Controles sobre la captura en línea.

Algunos de los principales controles en este tipo de captura son:

- Verificación de las transacciones individuales.

- Verificación de grupos de transacciones.

- Controles interactivos.

2.4.8 CONTROLES DE PROCESO.

Asegurar la exactitud del proceso de la información por el computador.

Identificar a través de una referencia única los datos que ingresan al computador para ser grabados junto con la información del registro.

Verificar que existan totales de control antes y después de procesar los registros a fin de tener la evidencia suficiente de la actualización de la información.

Verificar que se tengan herramientas de apoyo que garanticen que la integridad de la actualización de la información se realizó satisfactoriamente con los registros ingresados.

Reporte de transacciones.

Asegurar que se emitan los reportes de transacciones procesadas para verificar que fueron correctamente procesadas.

Verificación de transacciones.

Realizar validaciones adicionales a la numérica, alfabética o de rangos.

- Verificar que las transacciones lleven secuencia válida.

- Verificar contradicciones internas.

- Verificar que el proceso lleve una secuencia lógica.

Controles de la alta gerencia. (reporte de excepciones)

Verificar que se puedan emitir reportes para la gerencia en donde se indiquen desviaciones que sobrepasen límites significativos.

Controles en la integración de los sistemas.

Evaluar la confiabilidad de los procesos internos de todos los sistemas en conjunto, como es la transferencia de información entre sistemas.

2.4.9 AUTORIZACIÓN Y CONTROLES DE SALIDA.

Asegurar que toda la información que se procesa está debidamente autorizada y que existen controles sobre el acceso al computador, ya sea para obtener información o para modificar alguna transacción.

Las salidas del computador deben ser completas y confiables, así como ser debidamente distribuida, revisada y archivada.

Verificar que los niveles de seguridad que requieren los archivos para ser accesados sean los autorizados por la gerencia.

Asegurar la restricción al acceso a la información a través de las claves de acceso al computador.

Verificar que las claves de acceso se cambian periódicamente.

Establecimiento de huellas o pistas.

Asegurar lo adecuado de las huellas o pistas en la transformación de la operación.

2.5 AUDITANDO CONTROLES GENERALES.

La auditoría de los controles generales se encuentra ubicada entre las normas de ejecución del trabajo en el estudio y evaluación del control interno.

Los controles generales se aplican a todos los procesos en forma global que se llevan a cabo en una área de Procesamiento de Datos.

La auditoría de controles generales se puede llevar a cabo siguiendo las siguientes fases:

Primera fase.- Estudio Preliminar.

El objetivo de este paso es reunir antecedentes para identificar los procedimientos de control de aplicación específicos en la entrada, proceso y salida de la información por cada aplicación a sus diferentes sistemas, que deberían estar definidos por la organización auditada de acuerdo a sus características.

Asimismo, se debe obtener la descripción del equipo de cómputo, incluyendo datos tales como capacidad de memoria, sistema operativo, base de datos, comunicaciones, capacidad de dispositivos electromagnéticos, dispositivos de entrada, proceso y salida, teleproceso, etc.

Segunda fase.- Ampliación del estudio del control interno.

Documentar los controles generales.

El objetivo de este paso es el de adquirir información tomando en cuenta los controles generales, tales como:

- La organización estructural del centro de cómputo.

- Documentación de acuerdo a los estandares establecidos para el análisis, programación, prueba de datos y mantenimiento de sistemas.

- Verificación de la información procesada este sujeta a controles que aseguren que dicha información es válida, completa y debidamente autorizada.

- Revisión de los estudios de viabilidad para la adquisición de equipos así como la comprobación de manuales operativos actualizados de operación del equipo y de sistemas de operación, manuales para los usuarios, además verificar la existencia de copias de los manuales operativos y para usuarios.

- Verificación del adecuado uso de los controles sobre la bitácora.

- Evaluación de los controles contra contingencias y verificación de controles que aseguren la continuidad de la operación y contar con equipos de soporte y procedimientos de reinicio.

- Comprobar que la documentación de soporte de los programas esté n sujetos a los estándares establecidos, así como la existencia de controles para la protección de las copias de los mismos y de los archivos.

- Comprobar la seguridad física del centro de cómputo.

Tercera fase.- Pruebas a los controles generales.

El objetivo de este paso es determinar si los controles existentes están funcionando efectivamente.

Esto se logra aplicando procedimientos de auditoría.

- Determinar los procedimientos de auditoría para lograr un conocimiento detallado de los sistemas.

- Evaluación de que los controles de aplicación establecidos sean los adecuados.

- Seleccionar las pruebas de cumplimiento para probar los controles de aplicación establecidos en los programas y evaluar los resultados de las pruebas de cumplimiento para determinar si cumplieron con los resultados esperados y así comprobar si los controles funcionan.

Tercera fase alterna.- Pruebas a los controles generales para incrementar la eficiencia en los resultados de auditoría.

Finalmente el auditor debe decidir si se puede depender de los controles generales, es decir, evaluar sus fortalezas y debilidades identificando el impacto que estos tienen en el cumplimiento de control.

3. AUDITORÍA AL DESARROLLO DE SISTEMAS DE INFORMACIÓN.

En este apartado se hablará de los sistemas de información y de los aspectos que se deben tener obligatoriamente en una organización para ser revisados por un auditor en informática, ya que en la actualidad sucede que una organización tiene un departamento de procesamiento de datos el cual carece de los elementos necesarios para su evaluación.

Es por ese motivo que para llevar a cabo una auditoría al desarrollo de sistemas de información, el auditor debe tener a su disposición información referente a:

- Los objetivos del departamento de procesamiento de datos .

- Las principales funciones descritas y documentadas con su correspondiente definición de actividades y responsabilidades.

- Los programas de desarrollo de los empleados y escalafones, así como los programas de entrenamiento y evaluaciones de eficiencia del personal.

- La conformación de un Comité de Revisiones que participe en todos los asuntos relacionados con la Gerencia de procesamiento de datos.

- El documento descriptivo de las instalaciones disponibles para el procesamiento de datos, la documentación relativa a la adquisición del equipo y los planes de seguridad en las instalaciones y equipo.

- Documentación relativa a la adquisición, evaluación, control y seguridad de los sistemas de software, y los contratos de mantenimiento de sistemas de software.

- Documentación referente al proceso por medio del cual se describen los pasos lógicos estandar para desarrollar, programar, implementar y mantener aplicaciones de sistemas.

- Evaluación de proyectos respecto al costo-beneficio para ser desarrollado e implementado dentro de un marco definido de costos, tiempo y requerimientos técnicos y aceptación del proyecto por parte del usuario, con la capacitación recibida.

- Control de las modificaciones de las versiones a los sistemas implementados.

- Calendarios de trabajo para el personal de operación y procedimientos de control del procesamiento de datos.

Sin la disposición de esta información, el auditor no podrá proceder a efectuar su revisión debido a la falta de metodología para el desarrollo de los sistemas.

3.1 DEFINICIÓN DE SISTEMAS DE INFORMACIÓN.

Inicialmente se definirá el concepto de sistema para llegar a la definición de un sistema de información.

Se define el concepto de sistema de acuerdo al diccionario Larousse: "combinación de varias partes reunidas para conseguir cierto resultado o formar un conjunto."[11]

Se define un sistema de información como: "el conjunto de elementos, procedimientos íntimamente relacionados que tienen como propósito manejar datos, elabora reportes que permitan tomar decisiones adecuadamente para el logro de los objetivos de una empresa."[12]

Por lo tanto; se define un sistema de información para efectos de este trabajo de la siguiente manera:

El conjunto de elementos, procedimientos interdependientes, cuya finalidad después de la transformación de datos, es la de obtener información que va a ser la base para la toma de decisiones.

Para que el desarrollo de sistemas sea auditado, es necesario utilizar alguna metodología, a continuación se indican algunas consideraciones para establecer una metodología que todo sistema debe contener.

A) Investigación preliminar.

Entrevista con el usuario para la determinación de los requerimientos.

B) Determinación de los requerimientos.

Definición clara de las necesidades de los usuarios.

C) Antecedentes.

Descripción de como se lleva a cabo la actividad a sistematizar.

---

[11] *Larousse, Diccionario de la Lengua Española, tomo 1.*
[12] Gutiérrez J. José M. Apuntes.

D) Investigación y recopilación de información.

Obtención de la información necesaria para definir el alcance, objetivos y para llevar a cabo el análisis del sistema.

E) Definición y alcance del sistema.

F) Objetivos del sistema.

G) Análisis de costo/beneficio.

- Aprobación del usuario de la dirección de informática o del comité de sistemas.

I) Análisis estructurado.

- Elaboración de diagramas de flujo de datos lógico
(Debe incluir procesos, archivos, origen/destino de datos, flujo de datos y puntos de control.)

- Diccionario de datos.
(Descripción de los datos de entrada al sistema)

- Lógica de procesos.
(Utilizando árbol de decisiones pseudocódigo tabla de decisión.)

J) Diseño conceptual del sistema.

Debe incluir toda la fase de análisis estructurado, de diseño conceptual de los archivos, la estructura de lo datos, pantallas y reportes de salida.

K) Aprobación y firma del usuario y de auditoría.

L) Diseño detallado del sistema.

- Elaboración de diagramas de flujo detallado por módulo, estructura o menú.

- Diseño de archivos eliminando redundancia o estructura de datos.

- Diseño de pantallas y reportes de salida.

- Diseño de la seguridad de datos.

- Estándares para bibliotecas, menúes, procedimientos, programas, archivos, pantallas y reportes.

- Aprobación por parte de la gerencia de sistemas o de la dirección de informática.

- Definición de programas a desarrollar, asignación de recursos y calendario de trabajo.

O) Programación.

P) Presentación al usuario, debe incluir:

- Diagrama general del sistema
- Reportes que emite
- Medidas de control o seguridad con la que debe cumplir la aplicación.

Q) Integración de la documentación.
Manual técnico de operaciones y del usuario

R) Capacitación a los usuarios y personal de operaciones.

S) Instalación.

T) Mantenimiento al sistema.

Un sistema debe tener como características principales las de: Flexibilidad, adaptabilidad, modularidad, transferibilidad, mantenibilidad.

Tipos de sistemas de información.

Sistemas manuales de información.

En este tipo de sistemas, los datos son registrados manualmente con el uso del lápiz o pluma sobre documentos, empleando para ello caracteres numéricos y/o alfanuméricos.

Estos documentos son normalmente transferidos de un lugar a otro manualmente, puede se almacenado temporalmente en casillas o en forma permanente en archiveros. Cuando únicamente los procedimientos manuales son usados en un sistema de información, los errores pueden suceder fácilmente.

Como ventajas de estos sistemas es representativo el aspecto económico, la flexibilidad en cuanto a su operación y su fácil adaptación a posibles cambios, una de las desventajas es que encuadra a las personas en rutinas, que una vez conocidas y manejadas por largo tiempo, enajenan la actividad humana convirtiendo al individuo en una máquina y anulando su función primaria: la creatividad a través del intelecto.

Sistemas mecánicos de información.

Estos sistemas emplean dispositivos mecánicos que permiten un proceso de datos más eficiente. La recopilación de datos-fuente en este tipo de sistemas, se logra a través de mecanismos como máquinas de escribir, cajas registradoras, impresoras de cheques, relojes checadores, etc.

La transmisión de datos a corta distancia puede llevarse a cabo por medio de tubos neumáticos, interfonos, etc. A largas distancias, a través del teléfono, radios, correos, telégrafos, etc. Los documentos en sistemas mecánicos son almacenados en la misma forma que en los sistemas manuales, pero los datos contenidos en ellos estarán impresos o mecanografiados en vez de escritos a mano.

El cálculo sobre los datos puede ser hecho con máquinas propias para su propósito: calculadoras, máquina de contabilidad, para dar a conocer información procesada por estos sistemas, se usan máquinas de escribir, aunque también pueden usarse fotocopiadoras, etc.

El uso de dispositivos mecánicos puede incrementar grandemente la velocidad y exactitud de los procesos sobre datos, el proceso no es continuo ya que esencialmente se trabaja en forma manual, por lo tanto, se aprecia que las máquinas solo representan una ayuda para reducir las operaciones manuales en estos sistemas.

Sistemas de información electromecánicos.

Permiten el proceso de datos con mayor velocidad y exactitud que el sistema mecánico, en estos sistemas el volumen de operaciones puede ser incrementado sin aumentar personal o costos.

Algunas de las limitaciones de los sistemas electromecánicos son: el proceso no es continuo, ya que las partes de trabajo deben ser pasadas manualmente de máquina a máquina, los errores no pueden ser detectados con facilidad como es en los sistemas manuales, los datos manejados en sistemas electromecánicos deben por regla ser manejados en forma secuencial.

La principal característica de estos sistemas es la utilización de una codificación diferente a la escritura normal para manejar información, la información es simbolizada ya sea por marcas sensibles, caracteres ópticos o magnéticos.

Los datos contenidos en documentos fuente deben ser convertidos a una forma propia que permita su lectura y manejo por estas máquinas para que posteriormente se procesen los datos.

Sistemas electrónicos (Cibernéticos)

Cuando sean cuantiosos los volúmenes de datos a procesar, la complejidad de los procesos aumente, la velocidad de obtención de información requiera ser muy alta y el sistema demande por sus dimensiones estar totalmente integrado, se puede pensar que la solución para manejarlo esta dada por el uso de un equipo electrónico, una computadora.

Utilizando un sistema de cómputo electrónico, se pueden realizar operaciones como clasificar, reproducir, intercalar, calcular o tabular las cuales se realizan en forma integrada en un solo proceso y forma rápida.

Estos sistemas requieren menos espacio físico y menos personal operativo que en cualquier otro y precisan que los datos sean traducidos en impulsos que puedan ser captados por circuitos eléctricos los cuales estan articulados con dispositivos magnéticos que leen y graban datos.

La información en estos sistemas puede ser almacenada en medios magnéticos, el proceso lógico o matemático que realiza un computador, es efectuado en base a rutinas almacenadas en una parte de sus circuitos llamada memoria principal, estas rutinas son programadas por el hombre, por lo general por símbolos no legibles para la máquina y colocadas después de ser traducidas a un lenguaje propio de la computadora en la memoria principal de ésta.

Para procesar información en un computador, contamos con un equipo electrónico de proceso hardware y una serie de lenguajes y rutinas de soporte software. El equipo electrónico esta formado por uno o varios procesadores centrales y mecanismos periféricos electromecánicos (manejadores de cintas, discos, terminales, etc.) que serán la base mecánica de las operaciones. El soporte esta formado por rutinas y programas, desarrollas unos por el usuario y otro por la casa que fabrica el equipo, y servirán para ordenar al computador la forma en que deberá procesar todos los datos.

El procesador central de un computador electrónico desarrolla cálculos y procesos bajo el control de un programa almacenado.

El concepto de programa almacenado permite al computador escoger uno de varios cursos de acción, basados sobre datos de entrada o sobre resultados de un proceso previo, los cuales son pasados a través de un grupo de instrucciones ordenadas en un algoritmo. El mismo programa puede ser usado tantas veces como se requiera sin necesidad de que este sea reprogramado. Una vez instruido un computador, toma el control y se maneja automáticamente sin intervención humana los datos que le son

alimentados.

La información dada por un sistema electrónico es obtenida en forma de reportes impresos emitidos por impresoras de alta velocidad; también es posible obtenerla en desplegados visuales sobre pantallas o terminales.

Los sistemas electrónicos de información son diseñados para aplicaciones en los cuales grandes masas de datos deben ser recolectadas y analizadas, con el fin de reportar información significativa. Tales sistemas son también usados para manejar casos en los cuales los resultados de un proceso deben ser comparados para determinar reglas decisivas como una base para simples decisiones.

La alta velocidad de operación y la gran capacidad de almacenamiento de los sistemas electrónicos permite a estos manejar grandes volúmenes de datos y complejos procesos en forma económica y eficiente.

3.2 DEFINICIÓN DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN.

Se van a citar definiciones de auditoría de sistemas de información de distintos autores para ser analizadas en conjunción a la definición de auditoría informática que se presenta para fines de este trabajo, con la finalidad de aportar una definición que sea congruente al desarrollo de este trabajo.

Se cita la definición del C.P. Solis Montes: "Conjunto de técnicas y procedimientos que proporcionan al auditor los elementos de juicio suficientes para depositar confianza en la información procesada y contenida en los registros contables que se encuentran almacenados en dispositivos electromagnéticos o impresos en listados emitidos por la computadora"

Ron Weber dice: "Es el proceso de recopilar y evaluar la evidencia para determinar si se salvaguardan los activos, se mantiene la integridad de los datos, se logran las metas organizacionales y se aprovechan los recursos en forma eficiente"

También la Fundación de auditores del procesamiento electrónico de datos, proporciona la siguiente definición: "La auditoría de sistemas de información comprende cualquier auditoría que incluya la revisión y evaluación de todos los aspectos (o cualquier porción) de procesamiento por medio de sistemas de información automatizado, incluyendo los procedimientos manuales relacionados y sus interfases. Generalmente, el propósito de dicha revisión es valorar hasta que punto dichos sistemas o componentes que proporcionan información veraz y precisa y determinar si dicha información cubre las necesidades administrativas de la empresa y los aspectos legales

aplicables, en su caso."

Estas definiciones coinciden principalmente en la idea del mantenimiento de una integridad de datos adecuada para que el sistema proporcione información veraz y precisa.

Sin embargo la auditoría que se propone en este trabajo es la auditoría en informática como ya ha sido definida en el primer capítulo, así como en las definiciones anteriores pretende mantener una integridad de datos y vigila que la información procesada sea confiable, veraz y oportuna, también se ocupa de supervisar desde el diseño de un sistema para establecer controles y efectúa evaluaciones técnicas y administrativas.

Por lo tanto, se aprecia que las definiciones anteriormente mencionadas cumplen con la revisión a un sistema de información automatizado motivo por el cual se continuará trabajando con el término de auditoría en informática.

3.3 PROCESO DEL CICLO DE VIDA DE UN SISTEMA DE INFORMACIÓN.

Este proceso describe las fases de desarrollo y operación a través de los cuales pasa todo sistema antes de ser reemplazado o volverse obsoleto.

Durante la fase operativa el mantenimiento que puede ser la corrección de errores, modificación y afinación, por lo que puede ser considerada como una tercera fase.

Análisis de sistemas.

Es una técnica que sirve para definir y modelar la información que necesita la empresa previa a la toma de alguna acción.

El análisis del giro de la empresa permite la identificación y definición de entidades dentro del sistema. Estas entidades son elementos de los cuales el negocio necesita guardar información sobre ellos, siendo la parte medular del modelo de datos, donde pueden ser las actividades principales del negocio.

El primer paso consiste en identificar estas actividades y formar una lista, para eliminar algunas entidades se aplican las siguientes reglas:

a) Es la entidad un resultado del sistema? Quiero mantener un registro de esta entidad?

b) Trate de asignar una clave a la entidad, si esto no es posible no puede ser una entidad.

c) Esta entidad esta contenida en otra o depende de otra?

Así como es necesario identificar las entidades existentes es indispensable entender en que forma se relacionan estas entidades.

Tipos de relaciones.

a) Uno a uno

b) Uno a muchos

c) Muchos a muchos

El resultado de la fase de análisis es un documento de la especificación del sistema el cual se puede llamar, especificación funcional, especificación para diseño, documento de requerimientos.

Diseño y construcción del sistema.

Diseño

Esta actividad puede dividirse en dos partes:

Diseño lógico

Diseño físico

El diseño lógico finaliza con la presentación de las especificaciones de lo que se espera que realice el sistema en términos accesibles para el usuario. El diseño físico consiste en tomar el diseño lógico y traducirlo en entradas, archivos, salidas y especificaciones de programas.

Programación.

Consiste en la codificación de programas, pruebas y depuración de los mismos hasta que cada programa trabaja en forma correcta.

Pruebas a los sistemas.

Es el proceso de verificar que los programas, al momento de ser unidos para formar un sistema, funcionen de acuerdo a las especificaciones originalmente planteadas.

Implantación.

Existen dos actividades que deben ser planteadas antes de que el sistema entre en operación.

La primera consiste en generar los nuevos archivos maestros con base en los ya existentes, la creación de archivos puede ser

una actividad que consume mucho tiempo y requiere de una planeación cuidadosa para garantizar la factibilidad, exactitud y totalidad de los datos.

La segunda actividad es que el paralelo o proyecto piloto utilice datos reales, los resultados del sistema actual como prueba de que el sistema opera correctamente.

Mantenimiento.

Una vez que el sistema ha sido liberado será necesario darle mantenimiento en los casos de:

- Descubrir una falla en el sistema

- Cambien los requerimientos del usuario

- Se presenten cambios externos

Evaluación.

Es necesario llevar a cabo una evaluación posterior a la implantación con el objeto de garantizar que el sistema cumple con los objetivos y que no existen problemas operativos que requieran ser resueltos.

Algunas de las fases más importantes a realizar en esta actividad son:

- Realizar auditorías a las salidas y registros del sistema.

- Reportar requisiciones del usuario que no han sido satisfechas.

- Registros del performance y utilización del sistema.

- Desarrollo y monitoreo de indicadores críticos.

- Verificar quejas del usuario referentes a la seguridad, integridad y procedimientos de recuperación.

- Efectuar capacitación adicional.

- Preparar reportes de post-implantación y planes de afinación.

3.4 AUDITORÍA AL DESARROLLO Y MODIFICACIÓN DE SISTEMAS.

Esta parte trata de la importancia y necesidad de la intervención del auditor en informática, tanto en las modificaciones a programas en producción como en el estudio, diseño y desarrollo de nuevos sistemas o aplicaciones.

El personal encargado de desarrollar los estudios para una nueva aplicación o modificación, por su misma formación profesional, no esta sensibilizado, en su mayor parte, a los problemas de control y pistas de auditoría, por lo cual es frecuente encontrar que si bien un sistema es muy eficaz desde el punto de vista operativo, (tiempo, oportunidad de la información, etc.) éste carece de los controles necesarios que permitan asegurar la información implicada en el mismo, omitiendo igualmente proporcionar los datos necesarios para estar en posibilidad de efectuar la supervisión y recuperación de información para efecto de auditoría que se necesitarán posteriormente.

Es importante señalar que para el auditor en informática, el momento ideal para intervenir en un sistema es cuando éste esta en sus etapas iniciales de concepción, los controles sugeridos por el auditor en informática serán menos costosos y cumplirán en una mejor medida su propósito.

El auditor deberá tener la habilidad para no sobrecargar un sistema con medidas de control, en función a los objetivos e importancia del mismo, por lo tanto, el auditor debe encontrar un perfecto balance entre controles, seguridad, oportunidad, costo-beneficio y eficiencia en un sistema.

Existe un efecto muy interesante al participar en esta área como sigue:

A mayor participación en el desarrollo y modificación de sistemas, se obtendrá:

- Mayor confianza en los sistemas que se encuentren en un ambiente de operación.

- Será menor el esfuerzo para obtener pruebas de los archivos magnéticos para efecto de auditoría.

Estándares de desarrollo.

Un aspecto muy importante es el uso de estándares para el desarrollo de sistemas, incluyendo la documentación producto de estos.

Los estándares tiene como objetivo el contar con sistemas que sean comprensibles y fáciles de mantener al seguir una metodología adecuada que deberá incluir:

- Lenguajes a utilizar
- Estructura de programación
- Diagramas de bloque y de flujo
- Simbología a utilizar

Como producto de cada sistema se deberá obtener las documentaciones siguientes:

- Manual del sistema que incluya los documentos que dieron inicio al proyecto, las definiciones de requerimientos, las soluciones propuestas, diagramas de bloque y flujo, interrelación de programas, descripción de archivos, frecuencia de proceso, periodo de conservación de la información y en general toda la información relevante sobre el sistema que facilite su consulta y comprensión.

- Manual de operación orientado al personal de operación que incluya: una serie de procedimientos a seguir para procesar algún sistema incluyendo los controles previos y posteriores para validar la información y los posibles mensajes de error con sus respectivas acciones a tomar para reiniciar los procesos.

- Manual del usuario que incorporará la serie de pasos que éste tendrá que realizar para la preparación de los documentos y para su utilización una vez que han sido procesados.

Objetivos de la participación de auditoría en informática.

Los objetivos particulares que persigue ésta área de participación son los siguientes:

a) Valorar la suficiencia de los controles incorporados tanto en los programas como en los procedimientos previos y posteriores al tratamiento automatizado por parte de los usuarios que aseguren el nivel de confiabilidad deseado.

b) Validar la adecuación del sistema en relación a la oportunidad de la conversión y al costo beneficio en la implantación.

c) Verificar que el sistema sea comprensible, tanto para los usuarios como para terceras personas que eventualmente pretendan manejar el sistema.

d) Validar que el sistema sea auditable, incorporando dentro del mismo los datos necesarios para estar en posibilidad de recrear una operación desde su inicio hasta su fin (pista de auditoría) conservando por otra parte, la formación del tiempo necesario para esto.

e) Verificar que tanto las políticas internas de la empresa como las externas a ella sean respetadas.

Analizar la flexibilidad del sistema.

Se tratarán cuatro técnicas de auditoría que le servirán al auditor para alcanzar los objetivos que persigue. Se incluyen

ventajas para permitir al auditor decidir sobre la oportunidad de su aplicación.

1. Auditoría de Post-instalación.

Esta técnica describe los procedimientos estándares y formales que se deben llevar a cabo al examinar las aplicaciones una vez que éstas se han liberado en una producción normal. El hecho de haber incorporado algunos controles durante el desarrollo del sistema no garantiza que vayan a funcionar adecuadamente una vez que se encuentre en operación.

Esta técnica proporciona un método adecuado y sistemático para que los auditores examinen la efectividad de estos controles en un ambiente operacional.

El objetivo de esta técnica es verificar el apego y cumplimiento de políticas y procedimientos y determinar si el sistema está obteniendo los resultados para los cuales fue desarrollado.

Esta técnica no se limita a los programas de computador sino que incluye las interfaces manuales a través del sistema por lo que cubre todas las operaciones desde la preparación del documento fuente hasta la utilización de las salidas reflejadas en reportes, en consecuencia, ésta técnica incluye las funciones manuales relativas al sistema.

El alcance de la auditoría de post-instalación puede ser extenso o bien limitado dependiendo de los objetivos de Auditoría, en cualquier caso estos objetivos deberán ser definidos previo al inicio del trabajo.

2. Guías de control para utilizarse durante el desarrollo del sistema.

El momento ideal para el auditor para incorporar controles en una aplicación de computador, es durante la fase de desarrollo del sistema. Durante esta fase, los cambios y adiciones al sistema de control interno pueden ser realizados con un costo y un esfuerzo considerablemente menor, no así cuando el sistema se ha liberado.

La participación del auditor en la fase de diseño, pretende asegurar que el sistema de control interno especificado por el analista proporciona confianza en la integridad de la aplicación.

En este trabajo es de vital importancia que el auditor conserve su total independencia por lo cual éste no depende estructuralmente de los líderes de proyecto y no especifica

controles, sino que revisa y hace recomendaciones para mejorar el nivel de control planeado.

Se puede tener como apoyo guías de control que indiquen el marco de referencia en el cual se deben enmarcar los sistemas institucionalmente.

El auditor al revisar los controles del sistema durante las etapas de desarrollo, tiene la oportunidad de interactuar con los diseñadores del sistema cuando es menos problemático y costoso el realizar cambios. La auditoría tradicional solicitará una revisión una vez que el sistema ha sido liberado lo que ha probado ser demasiado costoso en la eventualidad de cambios a sugerencia del cuerpo de auditoría.

El auditor recibe copias de la documentación del sistema, participa en las juntas de trabajo del cuerpo de desarrollo y tiene la oportunidad de sugerir controles y modificaciones.

Las guías de control tienen dos ventajas:

- Ayudan a asegurar que el grupo de desarrollo incorpora controles importantes para la empresa.

- Ayudan a evitar las interrupciones y gastos de modificaciones una vez que el sistema se encuentra en producción.

3. Ciclo de vida del desarrollo de sistemas.

Esta técnica codifica la estructura intrínseca del proceso de desarrollo de sistemas en fases, e identifica puntos de control de calidad al final de tareas críticas en las fases.

En estos puntos los auditores observan y evalúan el avance y los productos para asegurarse de la auditabilidad del sistema y de que los controles previstos son adecuados y han sido ejecutados de la misma forma.

Las fases del ciclo de vida del desarrollo de sistemas han sido explicadas en el punto 3 de este capítulo.

4. Grupo de control y aceptación de sistemas.

Cuando el auditor determina probar y revisar el proceso de desarrollo de sistemas, se enfrenta al reto de cómo realizar de mejor manera esta revisión. A pesar de que la esencia de la revisión no cambia, el auditor en informática puede seleccionar entre la revisión al mismo o descansar en los esfuerzos de otro grupo.

Realizar la revisión por sí mismos, es la opción seleccionada por muchos auditores, a pesar de que se requiere de un entrenamiento y esfuerzo sustancial para hacer un buen trabajo. El hecho de que de este entrenamiento tiene que ver con procesamiento de datos en lugar de auditoría en informática, entre otros factores, llevado a utilizar un grupo especial de control y aceptación independiente de sistemas, que realizan revisiones sistemáticas para crear y mantener estandares efectivos de desarrollo, particularmente en la auditabilidad del sistema.

Este grupo forma parte del departamento de procesamiento de datos y su función es la de revisar y monitorear continuamente el desarrollo de aplicaciones significativas.

3.5 AUDITORIA A SISTEMAS EN OPERACIÓN.

Esta auditoría se da en los sistemas que ya se encuentran en operación. Estos sistemas pueden haber sido objeto de una intervención por parte del auditor en informática desde su inicio como proyecto, o bien pueden haber sido desarrollados sin ninguna intervención del mismo, por ser muy antiguos, por falta de coordinación de auditoría o por la ausencia, al momento de su desarrollo, de la función de auditoría en informática.

La auditoría de aplicaciones estará orientada a validar los resultados obtenidos a través de todo un sistema incluyendo tanto los usuarios como los programas mismos.

Es muy importante que el auditor reconozca el hecho de que un sistema y la serie de programas que lo conforman pueda ser vulnerable una vez que ya ha sido liberado en producción normal y puede, en un momento dado no estar procesando la información en forma adecuada y, en consecuencia no cumplir con los objetivos definidos inicialmente.

Es en esta área de participación de la auditoría en informática en donde se han desarrollado más técnicas a aplicar, ya que es aquí precisamente donde se encuentra el procesamiento de las operaciones que generan la información base para la toma de decisiones y afectaciones contables, por lo que cualquier error o manejo de éstas se traduciría en problemas y quizás en pérdidas para la organización.

Objetivos de la auditoría a sistemas en operación.

Los objetivos que persigue ésta área de la auditoría en informática son prácticamente los mismos que los citados en el punto anterior, validando que las medidas de control definidas dentro del sistema se mantengan a un nivel de confianza satisfactorio.

a) El objetivo general al auditar una aplicación es verificar que los procesos y controles incorporados en la misma la hacen confiable y que no existen puntos débiles que la expongan a riesgos significativos.

b) Verificar que los sistemas se encuentren trabajando de acuerdo a las especificaciones señaladas en la documentación del mismo, esto es que sean programas previstos, detectando programas "piratas" o bien que las modificaciones y utilización de nuevas versiones se encuentren perfectamente bien identificadas y documentadas para lograr esto el auditor en informática evaluará básicamente los tres tipos de controles:

Controles de entrada, Controles de proceso y Controles de salida, como ya se han citado en el capítulo anterior.

Al igual que en la Auditoría al desarrollo y modificación de sistemas, en este punto se mencionarán las técnicas desarrolladas para auditar ésta área señalando sus ventajas.

1. Método de datos de prueba.

Este método verifica la calidad del proceso al ejecutar los sistemas, utilizando grupos de datos de entrada especialmente preparados para obtener resultados preestablecidos.

Puede ser usado para probar y verificar:

- Rutinas de validación de transacciones de entrada, detección de errores y controles del sistema.

- Lógica del proceso y controles asociados con la creación y mantenimiento de los registros maestros.

- Rutinas computacionales, como intereses, pago bruto o depreciación de activos.

- Incorporación de cambios en los programas.

Sus principales ventajas son:

- Se obtiene evidencia objetiva, ilustrando la adecuación de los programas con las políticas, especificaciones y procedimientos de usuario establecidos.

- Se pueden hacer pruebas repetidamente utilizando juegos de datos establecidos para obtener resultados predeterminados.

- Se requiere de una ayuda mínima del grupo de procesamiento de datos para preparar los juegos de datos de prueba.

- Normalmente no se requiere de programación especial y los auditores requieren sólo de pocos conocimientos de procesamiento de datos.

2. Sistema de valuación de un caso de estudio.

Esta es una técnica que se utiliza para un grupo estandarizado de datos (entradas, parámetros y salidas) para la prueba de un sistema.

El caso de estudio, se define por el personal usuario, con la participación del auditor, como el criterio para el correcto funcionamiento del sistema.

Un caso de estudio se establece cuando se han procesado suficientes transacciones en la aplicación para asegurarse que todas las funciones de los programas han sido ejecutados, por lo que se puede decir que además de ser una técnica de prueba de auditoría, es una técnica de prueba de sistemas por la participación del usuario, la cual deberá incluir:

- Uno o más archivos que contengan la información necesaria para probar las condiciones válidas o inválidas, establecidas en el diseño del sistema (y modificaciones subsecuentes).

- Un grupo de transacciones de entrada predefinido que se diseña para probar cualquier eventualidad durante el proceso.

- Una salida predefinida para cada transacción probada.

- Un procedimiento manual o automático para comprobar todos los archivos y reportes para identificar cambios.

- Para sistemas en línea el caso de estudio debe incluir transacciones que contengan aquellas actividades normalmente realizadas en las terminales.

Ventajas:

- El departamento usuario participa en todas las fases del proceso de desarrollo o modificaciones; lo cual permite una validación más a conciencia durante su etapa de diseño y en consecuencia el sistema se apega más a las necesidades del usuario.

- La documentación de los sistemas es normalmente superior. El caso de estudio es una documentación en si misma.

- La responsabilidad de establecer y mantener la funcionalidad e integridad del sistema descansa en el usuario.

- El caso de estudio mejora sensiblemente la auditabilidad del sistema, ya que el auditor podrá utilizar el juego estandar de datos de prueba con resultados predefinidos para probar el sistema.

3. Prueba integrada.

Es una técnica que revisa aquellas funciones de una aplicación automatizada que son internas en el computador.

Los datos de prueba del auditor son utilizados para comparar los resultados del proceso de la prueba integrada en base a resultados.

Esta técnica permite al auditor examinar el proceso de una aplicación en su ambiente normal de operación. Utiliza una entidad ficticia dentro del marco de referencia del ciclo de procesamiento normal.

Se describe como integrada, porque las transacciones de auditoría son procesadas con transacciones en producción. Los registros maestros residen en los mismos archivos y la entidad ficticia se establece como parte de la estructura organizacional.

Ventajas:

- Provee un medio comprensivo de prueba de aplicaciones tanto para los auditores como para el personal de desarrollo sin ningún requerimiento especial.

- La selección se implanta como un programa de aplicación independiente en el cual las transacciones utilizadas como entrada a los archivos de producción son subsecuentemente procesadas por el programa de selección de auditoría.

- Bajo este concepto el auditor puede examinar y analizar un gran volumen de transacciones, a partir de muestras específicas, estableciendo por otra parte la frecuencia de errores en el trámite de las transacciones normales de la empresa.

4. Rutinas de auditoría implantadas.

Esta técnica utiliza uno o varios módulos de auditoría implantados dentro de los programas normales de la aplicación, estos módulos son insertados en los puntos del programa determinados por el auditor, señalando los criterios de selección, una vez que se obtienen los datos, se pueden utilizar métodos automáticos o manuales para analizarlos.

5. Paquetes generalizados de auditoría.

Es la técnica más ampliamente difundida para auditar aplicaciones de computador, permite al auditor analizar en forma independiente un archivo producto de una aplicación, la mayor parte de estos programas paquete de auditoría son muy confiables, altamente flexibles y muy bien documentados.

Normalmente esta técnica es usada para probar datos de archivos, actualmente se puede trabajar con este tipo de paquetes en sistemas en línea.

Las funciones básicas que tienen la mayoría de los paquetes son:

- Verificación de totales y totales cruzados.

- Selección y presentación detallada de datos tomados de un archivo.

- Realización de varias operaciones de lógica en los datos.

- Muestreo estadístico y extracción de información.

PRACTICA

I. Introducción.

Es importante que para la mayor comprensión de los temas antes citados en este trabajo de investigación, se alimenten los conocimientos con el desarrollo de una práctica profesional en un ambiente de trabajo informático, en donde el objetivo de la Auditoría a aplicar se cumplirá con el apoyo de una metodología de revisión general a la función informática.

Por lo que esta auditoría es de caracter Integral, ya que su campo de acción permite dar apoyo a la Alta Dirección, ser específica en el análisis de las areas de operación, programación, instalaciones de los equipos en las areas de trabajo, la paqueteria utilizada, los lenguajes para el desarrollo de sistemas, además evalúa el perfil del personal y en si la administración misma de la función.

Al final de la Auditoría Integral se plantea la problemática para dar pauta a recomendaciones y sugerencias a la alta Dirección, buscando lograr mayores beneficios dentro de la empresa y fuera de ella.

Es por este motivo que se solicitó practicar una Auditoría Integral a una División de Informática como parte de una prestigiada Firma Internacional de Contadores Públicos, y que prestó todo su apoyo para llevar a cabo esta tarea, la cual se describe a continuación.

II. Antecedentes.

Se praticó la Auditoría a una División de Consultoría Externa de una reconocida firma de Contadores Públicos. (Anexo I)

Su objetivo es el desarrollo de sistemas para proporcionar soluciones que le orienten a conducir al público usuario sus acciones, de esta manera contribuir al desarrollo de la productividad en las empresas a base de un proyecto continuo, en el que previamente se establecen objetivos y políticas para conceptualizar bajo el principio de costo-beneficio, finalmente promover la eficiencia con métodos idóneos, para un mejor desarrollo y un mejor aprovechamiento en los recursos.

Esta empresa fue creada hace tres años, su personal lo integran veintiseis elementos.

Director General.

Contador General

Jefes de análisis

Jefes de operación

Supervisores

Programadores

Sus departamentos son: (Anexo II)

Director General

Contador General

Gerente de Promoción

Desarrollo de sistemas

Estudios de viabilidad

El equipo de computo esta formado por: (Anexo III)

Tres microcomputadoras

Una IBM PS2

Un server con dos estaciones de trabajo

Una impresora lasser

Una impresora Star X-1500

Una PC para pruebas a los sistemas

Un modem

Sus aspectos generales son:

Sectores que atiende:

Industrial

Comercial

Bancario

Transporte

Construcción

Alcance a nivel nacional e internacional:

Su administración es:

En base a Presupuestos de los diferentes proyectos.

Presupuesto (tiempo y costo)

Los sistemas de apoyo a la Administración son:

- Evaluación del avance del personal.
- Control de habilidades para asignación de proyectos.
- Sistema de recuperación de información en caso de siniestros.
- Agenda de actividades.
- Sistema de control de proyectos.

Los lenguajes de desarrollo son:

- Dbase III Plus
- Clipper
- Lenguaje C
- RPG
- Cobol

III. Objetivo de la auditoría.

Efectuar una Auditoría Integral a la función informática y evaluar los controles en cada área para proponer recomendaciones y sugerencias que mejoren los controles ya existentes o sugerir nuevos controles.

IV. Metodología.

El presente trabajo se desarrolla mediante la siguiente metodología:

a) Test Deck de revisión para las áreas de Informática que son: (Anexo IV)

Gerencia

Sistemas y programación

Operación

Instalaciones

b) Desarrollo y evaluación de cada área a través de:

Investigación documental

Observación

Entrevista

Obtención de evidencia

c) Observación detallada del control.

Controles Gerenciales

Sistemas

Operación

Instalaciones

d) Problemática y recomendaciones

e) Evaluación de la auditoría integral

f) Conclusiones

V. Desarrollo de la metodología.

Es importante describir la forma en que se efectuó la revisión y expresar las facilidades que se otorgaron al personal dedicado al cumplimiento de esta labor, por lo que se ennumeran las actividades que se desarrollaron.

1. La práctica se efectuó en las instalaciones de la Empresa.

2. Un grupo de cinco personas llevó a cabo la aplicación de los test deck a las diferentes áreas de informática.

3. En el transcurso de las entrevistas y aplicación de test deck, fue importante observar la documentación de la empresa, los archivos confidenciales y el acceso inclusive a los sistemas.

4. Se tuvo el acceso a todas las oficinas de la empresa, y la documentación existente en cada una de ellas.

5. Se observó físicamente el equipo instalado, las conexiones de los cables, el lugar adecuado para el equipo, el cuarto de sistema eléctrico.

6. Se fueron obteniendo evidencias comprobatorias de la existencia de los controles motivo de revisión.

7. En algunos casos las evidencias se encontraban en diskettes.

Después de esta breve introducción al desarrollo de la investigación, se hará referencia a los resultados obtenidos en la aplicación de los test deck apoyándose en la observación detallada de los controles, investigación documental, entrevista y obtención de evidencia, para que de esta manera se indique la problemática existente y las recomendaciones que permitan la solución más óptima, y estimar los porcentajes de evaluación en cada area revisada y de esta manera dar resultados a la Alta Dirección para la toma de decisiones.

I. Respecto a los Controles Gerenciales, observamos lo siguiente:

Planeación.

Se afirma que los objetivos de la empresa auditada son acordes a una adecuada planeación de las actividades que se desarrollan a corto y largo plazo, los que incluyen cambios de organización, avances tecnológicos y requerimientos legales, asi mismo ubica los recursos apropiados para complementar los objetivos específicos de la Empresa.

La Dirección revisa periódicamente el avance eficiente de los objetivos obtenidos.

En el requerimiento del usuario, la Dirección participa en el diseño, pruebas e implementación de sistemas, para cubrir las necesidades del usuario, y asegurar el buen funcionamiento del sistema desarrollado por personal de la Empresa.

La Empresa cuenta con un plan de recuperación en caso de desastres, que consiste en un sistema que actúa de acuerdo al siniestro y se actualiza segun últimas versiones, el cual se prueba periódicamente para asegurar su buen funcionamiento, se guarda una copia del sistema en la Oficina Corporativa.

Organización.

No existe una estructura de las funciones que se desarrollan de acuerdo a las actividades que se efectúan en cada proyecto, ya que de acuerdo a las características del proyecto se selecciona a la persona responsable de éste.

Administración.

La Dirección General tiene políticas y procedimientos previamente documentados de acuerdo a las funciones que se deben desarrollar por cada uno de los integrantes de la División.

Se tiene un control efectivo sobre el desarrollo de los sistemas conforme a los tiempos de trabajo para la terminación de un proyecto.

Las políticas y procedimientos se mantienen al corriente y son comunicadas al personal.

Recursos Gerenciales.

Existe un documento que describe las instalaciones disponibles para el procesamiento de datos, al igual que un plan documentado para satisfacer requerimientos futuros.

Se realizan estudios de viabilidad para la adquisición de equipo, autorizados por el Director General, los cuales son aceptados mediante un estudio de justificación.

Se observó que la empresa no ha solicitado el contrato de mantenimiento preventivo para todo el equipo.

Administración del personal.

Se constató que todas las funciones que realiza el personal en el desarrollo de sistemas, esta documentada y actualizada.

La empresa cuenta con programas de desarrollo y rutas de ascenso para los empleados.

La selección de personal va de acuerdo al perfil del puesto requerido y con su respectiva investigación socio-económica.

Existen programas de educación contínua para el desarrollo y selección del personal, los cuales se actualizan cada seis meses.

El desarrollo de trabajo efectuado, se evalúa periódicamente de acuerdo con un sistema de evaluación computarizado.

Revisiones

Existe un Comité de Revisiones, el cual se encuentra organizado de manera informal, integrado por el Director General, la encargada administrativa y el analista en caso de requerirse.

II. Respecto a los Sistemas y programación. observamos lo siguiente:

Diseños y desarrollos.

El Director General es el encargado de definir los proyectos junto con los usuarios, en donde documentan los objetivos y el alcance del proyecto deseado.

Las firmas de aprobación por parte de la Empresa y usuarios no se encontraron, sin embargo existe la evidencia de que el proyecto fué autorizado.

Se observó el análisis documentado de los sistemas actuales los cuales evidencían los estudios de costo-beneficio para su adquisición.

La asignación del personal para el desarrollo de un proyecto, es de acuerdo a las características del proyecto, para esto se apoyan un sistema de control de habilidades para la asignación de proyectos, en donde el Director General decide a quien asignar.

El personal analista en ocaciones es el responsable del proyecto y en otras es el subordinado, lo cual quiere decir que el personal esta capacitado para enfrentar cualquier problema.

Diseño de detalles.

La Empresa estableció una definición estructural de los archivos de datos que intervienen en el sistema y asi mismo muestra documentados los formatos de entradas y salidas de información.

Se tiene la documentación de la descripción del equipo periférico y requerimientos de horario.

Existe un plan de conversión del sistema antiguo al nuevo sistema, el cual permite la legibilidad y entendimiento para cualquier persona o usuario.

Se tiene definido un plan de pruebas para cada sistema.

Control de proyectos.

El control de proyectos es automatizado mediante un sistema que ayuda a determinar los costos, ahorros, beneficios y métodos de procesamiento esperados por el nuevo sistema.

El Director General a través de este sistema mide el avance del proyecto de acuerdo a sus especificaciones y sobre el tiempo y costos contratados.

Programación.

Se verificó que la programación satisface las especificaciones del diseño de sistemas y que los programadores son acordes a los estandares de programación.

Se revisó la documentación de los programas encontrando la definición de los objetivos y propósitos del sistema a desarrollar, la descripción de los archivos usados y funciones que ejecutan, los diagramas de flujo de los pasos generales en el procesamiento de datos.

Los paquetes de documentación no contienen una lista del contenido, sin embargo, es un procedimiento general que se efectúa en la recopilación de la documentación del sistema.

Validación y pruebas.

Se ejecuta el plan de pruebas predeterminado a los programas y sistemas para asegurar que el sistema es funcional, que los programas satisfacen los objetivos de procesamiento asi como todas las funciones del sistema y además son acordes a las necesidades de los usuarios.

El funcionamiento del sistema se prueba después de su implementación.

Los analistas preparan los programas de entrenamiento para usuarios previamente a la implementación del sistema.

Sistemas y programas existentes.

El responsable directo del proyecto posee una copia de los programas implementados, describiéndose en ellos el contenido.

El Director General controla en el sistema de control de proyectos además de los avances de desarrollo, las modificaciones a los sistemas.

No existe la aprobación formal en el cambio a los sistemas por parte del usuario, sin embargo, se les comunica y dan a conocer las modificaciones efectuadas.

Los programas cuentan con una clave de acceso lógica que solo conocen los usuarios, existen dos tipos de password, los de tipo operativo y los administrativos.

Se tienen procedimientos para que el personal pueda procesar el respaldo de programas en caso de que el programa original esté dañado.

Está restringido el acceso a la documentación de sistemas y programas ya que estos se encuentran en la oficina del Director General.

Los archivos de datos se protegen con respaldos fuera de la Empresa.

Todas las generaciones de archivos de datos se mantienen conjuntamente con la información suficiente de las transacciones para asi reintegrar las generaciones subsecuentes.

III. Respecto a la Operación se tienen las siguientes observaciones:

Horarios.

Los horarios de trabajo son revisados y actualizados por el Director General de la Empresa.

No existe un calendario donde se programen los periódos de mantenimiento del equipo debido a la falta del contrato de mantenimiento.

Procesamiento.

El departamento cuenta con procedimientos para que sean utilizados por el usuario al momento de introducir datos, dichos procedimientos son autorizados por el Director General.

El software de sistemas que se utilizan son: Clipper, Mant is for vax 2.1., Dbase III, sistemas de recuperación en caso de siniestro, sistema de presupuestos, control de personal, agenda de actividades.

El departamento cuenta con documentos sobre los procedimientos que deben utilizarse para mantener un control de datos.

Existen manuales de información acerca de lo que hacen los diferentes programas.

El sistema en general cuenta con un método para prevenir y detectar los errores en las cifras de control.

Se maneja la información en diskettes los cuales son identificados por los usuarios de acuerdo a una clave determinada.

Existe un control de todos los archivos que maneja el departamento para evitar que el usuario pueda tener acceso a cualquiera de estos archivos.

Se encuentra en ocaciones información pendiente de distribuir, quedándose a la vista y alcance de cualquier persona.

Se mantiene un registro de distribución de información de salida.

Almacenamiento de datos.

Se cuenta con procedimientos de mantenimiento para la protección de los programas.

Hay un control de registros para inventariar los archivos según su fecha de generación.

El departamento cuenta con procedimientos para la recuperación de datos.

Seguridad.

Existen claves de acceso al computador para la restricción a determinados programas o aplicaciones, previamente identificadas y asignadas según la responsabilidad.

Se tienen los procedimientos de respaldo de información, periódicos y por daños en programas originales asi como la recuperación de la información en caso de pérdida.

Los archivos de datos se protegen con respaldos fuera de la Empresa, en las oficinas corporativas.

Todas las generaciones de archivos de datos se mantienen conjuntamente con la información suficiente de las transacciones para reintegrar las generaciones subsecuentes.

IV. Respecto a las instalaciones, seguridad y control, observamos lo siguiente:

El Comité encargado del procesamiento de datos existe pero no se encuentra formalizado, sin embargo es el responsable de la supervisión y revisión de los resultados de la instalación del sistema.

Se elaboró un proyecto para la instalación del equipo siendo responsable el Director General en el cual se consideraron espacios, estructuras, consideraciones del medio ambiente, identificando las fases para su instalación y revisión en los avances del proyecto.

El tiempo que se llevó para la instalación del equipo fué considerado dentro de los límites de tiempo asignado al proyecto autorizado por el Director General.

La empresa cuenta con sistemas de seguridad que cubre riesgos y casos de siniestros naturales o sabotajes, en cuanto a la pérdida de datos, mensualmente envía los respaldos de información a la Firma Internacional.

Las instalaciones de la empresa se localizan en un edificio de oficinas, por lo que la única seguridad con que se cuenta en el acceso al mismo es un policía en la recepción en la planta baja, sin embargo en los accesos del estacionamiento no existe control.

En cuanto a los requisitos mínimos de seguridad contra incendios de acuerdo a los estandares generalmente aceptados según la Asociación Nacional de Protección contra incendios, no existe notificación alguna.

En la oficina del Director General es donde se guardan los manuales, los diskettes originales del software.

Selección del equipo (hardware), seguridad y control.

El área de informática es el encargado del estudio de los requerimientos y de la instalación del mismo por lo tanto, integran el Comité de Requerimientos de Equipo.

El Director General y la Delegada Administrativa, son los encargados de señalar los requerimientos que debe satisfacer el equipo.

Se comnprobó que el proyecto hecho por los responsables del departamento es autorizado por el Director General.

Existe una lista de proveedores y de sus cotizaciones.

El personal de la Empresa es el mismo para la operación de mantenimiento del computador.

Se verificó que la Empresa tiene detalladamente las especificaciones de equipo así como las cotizaciones efectuadas por los menos a tres proveedores.

El cálculo de los costos del equipo es elaborado por el mismo personal de la Empresa, eligiendo la mejor alternativa.

El Director General es quien aprueba el equipo elegido, notificando al proveedor seleccionado.

Se observó que la localización de dos computadoras no es adecuada ya que se encuentran en el pasillo de más tránsito.

La sala de cómputo no cuenta con un extinguidor y en general la Empresa no tiene las medidas necesarias en caso de incendio.

Se observó que la Empresa no cuenta con un sistema de apoyo en caso de fallas en el suministro de energía eléctrica.

El personal conoce el plan de recuperación en caso de desastre y sus procedimientos ya que tiene el acceso a esta información a través de diskettes.

No se tiene un contrato con el proveedor del equipo para el mantenimiento preventivo y correctivo del equipo.

Selección de sistemas de software, seguridad y control.

En el proyecto de implantación del sistema se tienen señalados los requerimientos del software, y el equipo necesario para la aplicación, este proyecto fué elaborado por los integrantes de la Empresa y el Director General.

La adquisición del software se realiza a través de la Firma Internacional en función de los adelantos tecnológicos, por lo que existe un análisis de costo-beneficio para las adquisiciones.

El personal del área es el único autorizado para hacer uso del software, sin embargo esto no está por escrito.

El personal asignado a la construcción de sistemas para su contratación se efectúan investigaciones especiales para mayor seguridad de la Empresa.

Los programas aprobados con que operan las máquinas, se tienen debidamente documentados.

Se tiene un registro de todos los cambios a los sistemas, por lo tanto hay documentación respecto al mantenimiento de los mismos de acuerdo a los estandares de la instalación.

La empresa cuenta con la metodología adecuada, estandar para desarrollar, documentar, implementar y mantener las aplicaciones de los sistemas.

INFORME DE CONTROLES GERENCIALES.

RECOMENDACIONES

1. Solicitar contratos de mantenimiento preventivo necesario para todo el equipo.

2. Estructurar las funciones de la empresa para el desarrollo de proyectos y a la vez establecer estandares reales de ejecución para cada tarea específica y sean conocidos por los empleados.

SUGERENCIAS

1. Sugerimos que por lo menos los servicios contratados sean por seis meses.

2. Evaluar los resultados del personal en la ejecución de sus tareas.

INFORME DE SISTEMAS Y PROGRAMAS

RECOMENDACIONES.

1. Establecer un registro de firmas para la autorización del proyecto por ambas partes, o bien un documento donde el cliente se hace responsable de aceptar el proyecto planteado por la Empresa y asi llevar un control y evidencia suficiente del mismo.

INFORME DE OPERACION

RECOMENDACIONES

1. Establecer el contrato de mantenimiento para protección de los equipos.

2. Los archivos de respaldo se deben guardar en un lugar fuera del departamento.

SUGERENCIAS

1. Contratar el servicio de mantenimiento, para establecer un calendario de trabajo considerando los dias correspondientes.

2. Se sugiere que la información se guarde en un lugar fuera del departamento.

3. Conservar en un lugar de fácil acceso al operador el instructivo de contingencias en caso de mal funcionamiento del equipo y además mantenerlo actualizado.

INFORME DE INSTALACIONES, EQUIPO Y SEGURIDAD FISICA.

RECOMENDACIONES

1. Es necesario que la empresa tome la decisión de restringir el acceso al personal no autorizado para evitar cualquier tipo de perjuicio en el equipo de cómputo.

2. Asignar un lugar más seguro para custodia de la información, asi como los programas que se encuentran en la oficina del Director General.

3. Colocar extinguidores en áreas visibles de fácil acceso.

SUGERENCIAS

1. Indicar por escrito el personal con acceso al equipo de cómputo.

2. Asi mismo indicar la distribución del personal para la utilización del software.

3. Practicar periódicamente auditorías al acceso del equipo.

4. Reubicar las dos computadoras que están en el pasillo, en un lugar menos transitado.

5. Instalar un no break.

Problemática y recomendaciones.

CONTROLES GERENCIALES.

Problema.- Los equipos no tienen un plan de mantenimiento preventivo.

Recomendación.- Contratar el servicio de mantenimiento preventivo por lo menos cada seis meses.

OPERACION.

Problema.- Los usuarios (analistas, programadores) no guardan en algunas ocaciones los diskettes de trabajo.

Recomendación.- Asegurarse que al final del día, los diskettes no se encuentren a la vista.

Problema.- Existen claves de seguridad para cada usuario en determinados proyectos los cuales no son verificados.

Recomendación.- Revisar periódicamente la bitácora auditora para revisar los accesos a los proyectos conforme su asignación.

INSTALACIONES, SEGURIDAD Y CONTROL.

Problema.- La instalación eléctrica se encuentra en un lugar de difícil acceso para su revisión y no está debidamente protegida.

Recomendación.- Cambiar la instalación eléctrica a un lugar de fácil acceso para su reparación o revisión.

Problema.- No hay una fuente de poder, no break, para asegurar la información en caso de fallas eléctricas.

Recomendación.- Adquirir a la brevedad un no break.

Problema.- Solo existen 4 computadoras para 18 programadores y analistas.

Recomendación.- Es necesario adquirir más equipos para evitar retrasos en el desarrollo de sistemas.

SISTEMAS Y PROGRAMACION.

Problema.- El equipo de cómputo está a disposición de los usuarios, lo que ha provocado que existan archivos sin utilizarse y aunque se efectúan las limpiezas de archivos, estas continúan en algunas áreas.

Recomendación.- Es necesario programar periódicamente la limpieza de archivos o bien crear un sistema software con el fin de tener áreas libres y no tener tiempos de respuesta tardados.

Problema.- El diseño conceptual queda documentado pero no firmado por la empresa ni por el cliente.

Recomendación.- Es importante recabar las firmas para evitar descontentos en la recepción y entrega de sistemas liberados.

Problema.- No se firman contratos por el tipo de servicio que la empresa vaya a proporcionar a su cliente.

Recomendación.- Es recomendable describir en la contratación de servicios el tipo de servicio que se proporcione.

- Desarrollo de nuevos sistemas.
- Mantenimiento.

EVALUACIÓN DE LA AUDITORÍA INTEGRAL

	OPTIMA	EMPRESA
CONTROLES GERENCIALES.		
PLANEACIÓN	30	30
ORGANIZACIÓN	20	20
ADMINISTRACIÓN DEL PERSONAL	20	20
RECURSOS GERENCIALES	15	15
REVISIONES	15	15
	100%/4=25%	100%=25%
INSTALACIONES, EQUIPO Y SEGURIDAD FISICA.		
SELECCIÓN DE INSTALACIONES	30	20
SELECCIÓN DEL EQUIPO HARDWARE	30	22
SELECCIÓN DE SISTEMA SOFTWARE	40	35
	100%/4=25%	77%=19%
SISTEMAS Y PROGRAMACIÓN		
DESEÑO Y DESARROLLO	10	10
DISEÑO DE DETALLES	15	15
CONTROL DE PROYECTOS	15	15
PROGRAMACION	10	15
VALIDACIÓN Y PRUEBAS	10	10
SISTEMAS Y PROGRAMAS EXISTENTES	40	35
	100%/4=25%	100%=25%

	OPTIMA	EMPRESA
	OPERACION	
HORARIOS	25	24
PROCESAMIENTO	25	25
ALMACENAMIENTO DE DATOS	25	25
SEGURIDAD	25	25
	100%/4=25%	99%=24%
T O T A L E S	100%	93%

ESCALA DE EVALUACION.

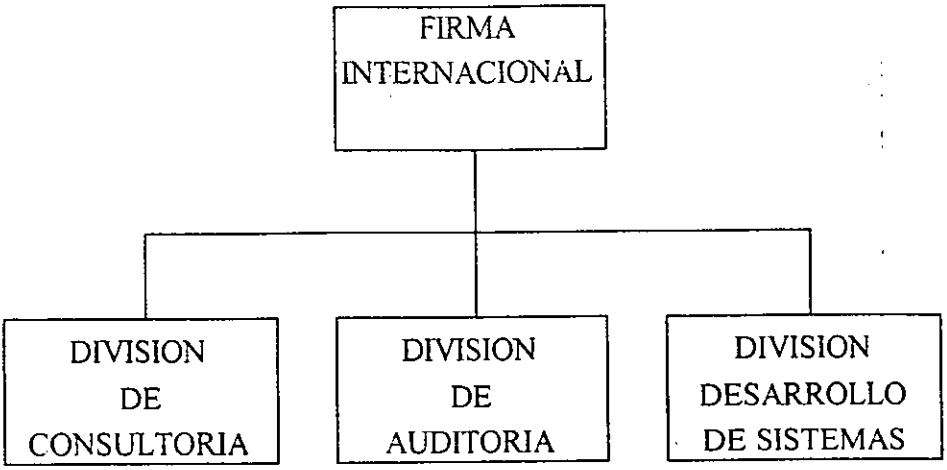
90 - 100	EFICIENTE
80 - 89	BUENO
70 - 79	REGULAR
60 - 69	ACEPTABLE
0 - 59	MAL FUNCIONAMIENTO.

CONCLUSIONES.

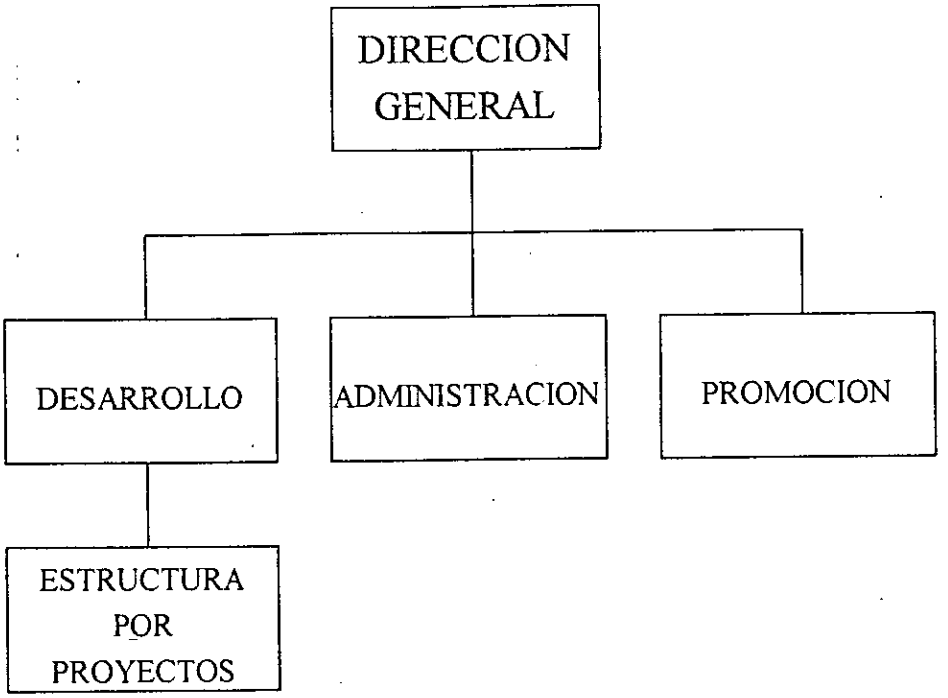
La empresa auditada es una empresa definida y autorizada en todas sus funciones en donde el cumplimiento de sus objetivos se realiza con el apoyo y distribución que existe en los recursos humanos, materiales y financieros, los cuales estan dirigidos y vigilados apropiadamente por la Dirección.

En términos generales, el desarrollo de sistemas es eficiente, contribuye al desarrollo de la productividad en las empresas, da confianza al beneficiario y además los sistemas se desarrollan sobre bases firmes y controladas, sin embargo, es susceptible de mejorarse tomando en cuenta nuestras observaciones y sugerencias.

ANEXO 1


FIRMA INTERNACIONAL
DIVISION DE CONSULTORIA
DIVISION DE AUDITORIA
DIVISION DESARROLLO DE SISTEMAS

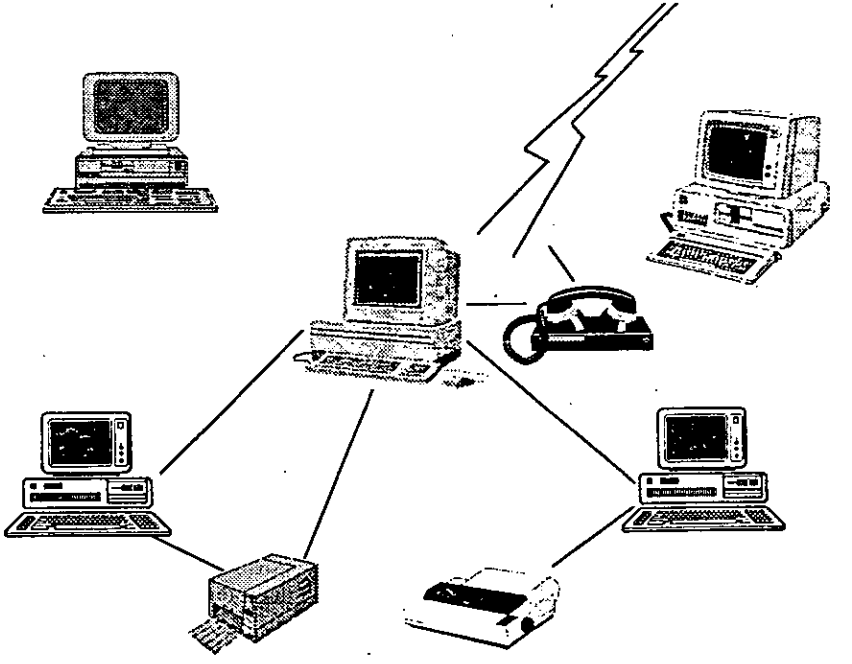
ANEXO 2


DIRECCION GENERAL
DESARROLLO
ADMINISTRACION
PROMOCION
ESTRUCTURA POR PROYECTOS

ANEXO 3

EL EQUIPO DE COMPUTO ESTA FORMADO POR:

- UNA IBM PS-2
- UN SERVER CON DOS ESTACIONES
- UNA IMPRESORA LASER
- UNA IMPRESORA STAR X-1500
- UNA PC PARA PRUEBAS A SISTEMAS
- UN MODEM



ANEXO 4

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS

PUNTO	DESCRIPCION	HECHO	COMENTARIO
1	PLANEACION Asegurar que las actividades del desarrollo de sistemas sean planeadas de manera que sus objetivos puedan obtenerse bajo una conveniente rel. costo-beneficio.		
2	Asegurar la existencia de los objetivos a largo plazo, este debidamente documentados, además comprobar que los planes sean dirigidos al cumplimiento de los objetivos a largo plazo.		
3	Verificar que los planes reconozcan los cambios futuros de la organizacion, avances tecnológicos y requerimientos legales.		
4	Habiendo conocido los planes que respaldan a los objetivos, verificar la ultima fecha de revisión en la obtención de los mismos y comprobar que los planes vayan acompañados del análisis costo/ben		
5	Verificar que esten definidos y aprobados los recursos asignados para la consecusión de los planes e incluyan planes de operación detallados.		
6	Verificar que se comparen los progresos obtenidos en los planes originales, en los planes de recuperacion en caso de desastre verificar la recuperación mediante la documentación existente.		
7	Comprobar que exista un Comite de Informática integrado por personal clave de todas las áreas usuarias y que sea el que establezca prioridades para la función.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
8	Evaluar las condiciones de trabajo para motivar la productividad de los empleados por entrenamiento, reconocimiento o reasignación de labores.		
9	Verificar la continuidad de evaluación de la gerencia y empleados para determinar que tan efectivamente se realizan las actividades y responsabilidades asignadas.		
10	Comprobar la existencia de estandares reales de ejecución para cada tarea especifica y sean conocidos por los empleados para su evaluación.		
11	Revisar que existan manuales de organización, politicas y procedimientos, actualizados y sean del conocimiento del personal y se apliquen.		
12	Verificar que los sistemas con periódos largos de desarrollo o presupuestos importantes estn bajo el control de proyectos de la gerencia.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
1	ORGANIZACION Y ADMINISTRACION. Verificar que la estructura orgánica del área de admon. y control de sist. en desarrollo este debidamente autorizada, vigente, con nivel jerárquico apropiado.		
2	Comprobar la existencia y vigencia de adecuadas descripciones de funciones y perfiles requeridos para cada área.		
3	Cerciorarse de que existan programas de adiestramiento y capacitación que permitan contar con personal calificado para el adecuado desarrollo de la función.		
4	Comprobar la última evaluación a los programas de entrenamiento en cuanto a calidad y costo y compararlos con fuentes alternativas de educación de personal.		
5	Verificar la definición de los programas de desarrollo de empleados y escalafones previstos y a futuro.		
6	Verificar que exista un análisis sistemático de cargas de trabajo que permita determinar la insuficiencia o exceso de recursos humanos y comprobar el cumplimiento de programas de ajuste de persona		
7	Revisar que se cuente con los recursos tecnicos y materiales necesarios para llevar a cabo la función, y comprobar que exista un documento que describa las instalaciones disponibles.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
1	INSTALACIONES, EQUIPO Y SEGURIDAD FISICA Verificar que las instalaciones de las computadoras son las adecuadas así como el uso y manejo de personal.		
2	Verificar que el Comite de Informática sea responsable de la iniciación, guía y revisión de resultados del plan de preparación de instalaciones.		
3	Verificar que los requerimientos de instalación identifiquen el ambiente necesario para la instación de los equipos.		
4	Comprobar la existencia gráfica de tiempos y fases de las instalaciones asi como la calendarización debidamente autorizados por la gerencia.		
5	Verificar que haya un plan de seguridad en las instalaciones por la destrucción o daños accidentales y sean previstos.		
6	Comprobar la actualización del plan de recuperación en caso de desastre sea preparado y ubicado en un lugar que permita un rápido acceso de salida de las instalaciones.		
7	Verificar el acceso restringido del personal al área de cómputo incluyendo acceso a las terminales y sea debidamente documentado		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
8	Verificar que las protecciones contra incendio en las instalaciones sean de acuerdo con los estandares generalmente aceptados como los que publica la Asoc. Nal de protección contra incendios.		
9	Comprobar la existencia de una instalación fuera de la empresa para guardar copias de sistemas, aplicaciones de programas, documentación y otros registros importantes.		
10	Verificar los estudios de costo/beneficio derivados de la introducción de equipo de cómputo para el procesamiento de la información.		
11	Verificar que la documentación del requerimiento contenga un reporte y diseños que debe satisfacer el equipo y comprobar la aprobación de la gerencia para la selección de equipos.		
12	Verificar que la documentación de los proveedores seleccionados, tengan especificaciones de sus equipos para ser sometidos a la aprobación según requerimientos de la empresa.		
13	Comprobar que la gerencia es quien aprueba la selección del equipo considerando las pruebas, conversión y procedimientos.		
14	Verificar que el personal de operación conozca el plan de recuperación en caso de desastre y sus procedimientos.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
1	OPERACION Verificar que exista y se ponga en práctica el manual de metodos y procedimientos de ejecución para los operadores de la computadora en los siguientes puntos:		
	- Encendido y apagado del equipo. - Acciones a adoptar en caso de fallas del sistema. - Tiempos estandar para montar y desmontar los dispositivos de almacenamiento.		
	- Descripción de las actividades prohibidas.		
2	Verificar que existan y se pongan en práctica las instrucciones para correr cada uno de los sistemas en producción y que se haya establecido el estandar de consumo de recursos normal.		
3	Comprobar que se han establecido los procedimientos tradicionales de control interno: rotación de personal, entrenamiento, programación de vacaciones, asignación de dos o más operadores.		
4	Verificar que se examinen periódicamente las actividades de los operadores a traves de los registros del sistema operativo y se supervicen las desviaciones importantes.		
5	Verificar que existan y evaluar que sean correctos los controles de uso del equipo de cómputo para correr sistemas en producción, reprocesos, actividades de desarrollo de sistemas.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
6	Verificar que se revisen periódicamente los reportes de los operadores sobre el mantenimiento preventivo y correctivo que se da al equipo, que se investiguen desviaciones y adopten medidas.		
7	Verificar que el personal que controla la recepción-entrega de datos a los usuarios, no tenga funciones de captura y procesamiento.		
8	Evaluar que los metodos y procedimientos implantados en la sección de control, sean adecuados de acuerdo con las caracteristicas de la información que entra y sale del procesamiento.		
9	Verificar que la sección de biblioteca cuenta con instructivos para: - Ordenar y mantener adecuadamente los archivos.		
	- Mantener un registro de cada uno de los archivos para identificarlos por nombre, programas y personal autorizado para utilizarlos y personal responsable del archivo, versión, requerimientos.		
10	Revisar y evaluar que los controles establecidos para la documentación de los sistemas, programas, manuales de los operadores y usuarios esten a disposición de personal autorizado.		
11	Verificar que se cuente con planes de recuperación en casos de desastre y revisar que contengan - Enumeración de los posibles riesgos para la instalación de cómputo y sus riesgos.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
	- Evaluar el funcionamiento del sistema a traves del rastreo de transacciones. - Identificar las consecuencias de error mediante el registro de quienes tuvieron acceso.		
12	Dada la magnitud de la instalación de cómputo y de los sistemas que manejan, verificar que existan archivos con la información de los eventos que ocurren al correr la aplicación.		
13	Verificar que todos los archivos del computador esten inventariados y controlados por registros apropiados además deben ser identificados de acuerdo a los estandares establecidos y protegidos.		
14	Comprobar que el personal de operación este familiarizado con los procedimientos requeridos para procesar en equipos de respaldo.		
15	Comprobar que existe un archivo de respaldo fuera del centro de cómputo sobre bases de rotación regular para todos los archivos de datos.		
16	Verificar que sean adecuados los controles y procedimientos que esten en vigor para proteger las operaciones del computador y los archivos de datos de modificaciones accidentales o deliberadas.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
1	SISTEMAS Y PROGRAMACION Verificar que el diseño y desarrollo de sistemas se lleve a cabo conforme a los objetivos establecidos en la planeación.		
2	Determinar si los recursos humanos y de cómputo disponibles permiten efectuar los planes de desarrollo de sistemas.		
3	Verificar que previamente al inicio del diseño de sistemas se realizaron y estan debidamente documentadas las siguientes actividades:		
	- Definición clara del problema a resolver. - Descripción de los objetivos del nuevo sistema, asi como de las limitaciones de recursos y de organización.		
	- Debe existir un análisis documentado y completo del sistema presente. - Tambien un resumen de costos del sistema actual y la certeza de que estos costos son adecuados		
	- Debe existir una definición de los nuevos requerimientos de información. - Debe existir un diseño conceptual preparado para el nuevos sistema.		
	- Debe existir un análisis de los usos estimados y de los costos del desarrollo de sistemas asi como los beneficios.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
	- Verificar la aprobación formal (firmas) de la gerencia, usuarios en la definición del proyecto.		
	- El estudio preliminar del sistema para evaluar la factibilidad de automatizar el sistema y que comprenda: la determinación de los recursos tecnicos, posibilidad de obtener datos, utilización		
	de los productos que se esperan, identificación del sistema en la organización y en los procedimientos del usuario, asi como la determinación de costos y beneficios que se obtendrán.		
4	Verificar que la definición de los requerimientos de entrada y salida esten debidamente documentados y la definición estructural del proyecto de archivos de datos base.		
5	Verificar las autorizaciones y firmas de la gerencia y usuarios sobre los puntos clave para medir el avance de los proyectos.		
6	Verificar que en el diseño de sistemas se consideren volúmenes de información a procesar en áreas de almacenamiento de información requeridas.		
	- Tiempos de respuesta - Facilidades de programación - Limitaciones de la integridad de los datos - Uso que se le dará a la información procesada.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
7	Verificar que se cuente con estandares para elaborar los programas de cómputo y evaluar que sean correctos de acuerdo con los recursos disponibles.		
8	Verificar que cada programa contenga la descripción de su propósito, archivos usados de entrada y salida, las funciones que ejecutan, diagrama de flujo a nivel macro, diseño de reportes.		
9	Comprobar que los programas se forman según los estandares establecidos.		
10	Verificar los procedimientos de control de la gerencia de desarrollo de sistemas para la revisión y aprobación de la documentación de los programas.		
11	Verificar que el sistema es completamente funcional y que todas las órdenes y lógica en los programas son diseñados de acuerdo a los requerimientos de los usuarios.		
12	Verificar que el diseño de procedimientos y formas asi como los manuales de los usuarios sean claros, precisos y estn de acuerdo con el diseño de sistemas		
13	Verificar si todos los controles estan funcionando bien, y comprobar la autorización del sistema para su implementación.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
14	Efectuar pruebas conforme al plan de pruebas predeterminado para comprobar que los programas se adhieren a los estandares de programación y dichos resultados son aprobados por la gerencia.		
15	Verificar mediante una prueba de sistemas que todas las funciones cumplan con el plan aprobado para la prueba de sistemas, se obtengan los resultados predeterminados y funcionen los controles.		
16	Verificar la documentación que respalde la revisión formal, evaluación y aceptación de los resultados de la prueba de sistemas por la gerencia y los usuarios.		
17	Verificar que se lleven a cabo las siguientes actividades previamente a la puesta en operación del nuevo sistema:		
	- Capacitación del personal usuario. - Capacitación del personal de sistemas en caso de que se hubieran cambiado o introducido nuevos recursos de cómputo.		
	- Conversión de archivos y programas al formato necesario para el nuevo sistema. - Calendarización de las operaciones y corridas de prueba.		
18	Verificar que antes de implementar el sistema los objetivos del nuevo sistema han sido conocidos y los usuarios han tenido el entrenamiento necesario.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
19	Verificar que el funcionamiento del sistema despues de la fase de conversión en los archivos maestros y tablas de decisión.		
20	Evaluar la corrección del proceso de conversión de los archivos maestros.		
21	Verificar que existe un proceso adecuado por el cual el desarrollo, documentación e implementación de cambios a los sistemas y programas existentes son controlados.		
22	Comprobar que los cambios a los sistemas y programas son controlados y aprobados por los usuarios.		
23	Verificar que se efectuen procedimientos de prueba para cambios a los sistemas y programas de acuerdo con los planes de prueba predeterminados y con estandares de pruebas.		
24	Verificar que existan procedimientos referentes a la aprobación de los usuarios en las pruebas a los sistemas y los resultados de los cambios sean de acuerdo a las necesidades del mismo.		
25	Verificar que han sido diseñadas las medidas de seguridad necesarias en los programas y sistemas, y que estan incluidas las señales de protección.		

TEST DECK DE LOS CONTROLES GENERALES DEL DESARROLLO DE SISTEMAS			
PUNTO	DESCRIPCION	HECHO	COMENTARIO
26	Comprobar que la aplicación de sistemas y programas reporten los intentos de accesos no autorizados.		
27	En los sistemas y programas existentes comprobar que los controles y procedimientos de seguridad se hayan incluido en su desarrollo y esten documentados en una área restringida.		
28	Comprobar que los programas operacionales se guarden en una ubicación fuera de las instalaciones		
29	Verificar que existan reportes periódicos que indiquen el uso de programas, incluyendo fechas, tiempos, frecuencias e individuos responsables de uso.		

B I B L I O G R A F I A

1.- Larousse, Diccionario de la lengua española, tomo 1.

2.- Normas y procedimientos de auditoría. Instituto Mexicano de Contadores Públicos, A. C.,1992

3.- Diccionario porrúa de la lengua española.

4.- Echenique, García, J. Antonio, Auditoría en informática, Mc Graw Hill. 1990.

5.- Boletín E02, control interno, Instituto Mexicano de Contadores Públicos, A. C.,1992

6.- Gutiérrez, Juvera, José Manuel, Apuntes.

7.- Código de ética profesional, Instituto Mexicano de Contadores Públicos, A. C.

8.- Hernández, Jiménez, Ricardo, Administración de centros de cómputo, ed. trillas, 1990.

9.- Paniagua, Victor, Auditoría integral, UNAM Facultad de contaduría y administración, 1987.

10.- Lazcano, Seres, Juan M., Auditoría e informática, Instituto Mexicano de Contadores Públicos, A. C.,1989

11.- Seminarios de excelencia en auditoría informática.

12.- Recopilación de conferencias perspectivas de la seguridad y la auditoría informática en los 90's en México, Compu-Com Internacional de México, S.A. de C.V.

13.- Apuntes UPICSA, licenciatura en informática.

14.- Boletín D430 Sistemas automatizados, SECODAM.

15.- Procedimientos de control en computación, I.M.C.P.

16.- Senn, James, Sistemas de información para la administración, Grupo Ed. Iberoamérica.