50680

Matrimonio Cruz:

Amigos.... grandes amigos...
Quisiera que quedara este momento
para parte del fuego de una meta de
un compromiso que siempre los guardara
en su corazón.

Los recordare Siempre

Joaquín Morales

2-03-90.

Atizapán de Zaragoza, Estado de México

Mayo 1990

A mi Madre:

Lucía del Carmen

con Gratitud, Admiración y Amor

A mis Hermanos:

Victoria, Sergio, Victor y Noé

con Respeto y Amor

Al Recuerdo de mi Abuelo:

Noé Valladares Martínez

A mis Primos:

Lourdes León de Colón

Horacio Colón Hernández

con Gratitud, Respeto y Cariño

A todos los que de una u otra forma
han contribuído a mi formación
profesional y en especial a:

C.P. Miguel Castro Aznar

C.P. Cecilia Sevilla Ramos

Ing. Emilio Alvarado Badillo

A mis Familiares y Amigos.

AGRADECIMIENTOS

Para la elaboración de un trabajo de investigación es necesario la asesoría de personas especializadas en el campo de su actuación profesional.

Quisiera transmitir a través de estas líneas el profundo agradecimiento que llevo en mi persona hacia el C.P. Gustavo Adolfo Solís Montes M. en C. y al L.S.C.A. Ralf Eder Lange M. en C. por su disponibilidad y el profesionalismo mostrado en el asesoramiento y dirección del presente documento.

GRACIAS

Joaquín Elías Morales Valladares.

INDICE

RESUMEN

"Conceptualización de un Sistema de Revisión de Controles Generales como herramienta de apoyo al Auditor de Sistemas de Información" es un trabajo de investigación que expresa en su contenido temas que son de importancia para el auditor de sistemas de información.

En sus capítulos I al IV se analizan, a través de un marco teórico, conceptos, fundamentos, procesos, objetivos, necesidades, elementos, impactos y procedimientos que integran o componen y en ocasiones afectan a la auditoría, a la auditoría de sistemas de información, al control interno y a los controles generales.

Este trabajo muestra el firme propósito de dar a conocer la importancia que tienen los controles generales en una auditoría de sistemas de información y al mismo tiempo conceptualizar un sistema que pueda convertirse en una herramienta útil para la revisión de estos controles; como podrá apreciarse en el capítulo V.

Para mostrar al final las conclusiones que como resultado de la presente investigación se obtuvieron.

INTRODUCCION

Los sistemas computarizados de información son desarrollados para satisfacer las necesidades de operación y de información así como dar soporte para la adecuada toma de decisiones en una organización.

El empleo de estos sistemas en los procesos administrativos y financieros es uno de los cambios más significativos en las organizaciones modernas.

Es pues necesario prepararnos ya que estos sistemas introducen nuevos riesgos al impactar los ya existentes en los sistemas manuales.

Debido a lo anterior y en vista de que los sistemas de información se convierten en una parte integral de la operación administrativa y financiera de la organización y que además se están volviendo mas extensos y complejos, surge la necesidad de diseñar bases especializadas de revisión de estos sistemas que permita soportar la confianza en los mismos.

OBJETIVO

Este trabajo nace de la inquietud de dar soluciones al auditor tradicional y al auditor en sistemas a través de conocimientos básicos y el uso de herramientas como lo es el sistema que se plantea.

Por lo tanto el propósito será el de contribuir con conocimientos básicos para capacitar al auditor en el estudio y evaluación de los controles generales y al mismo tiempo conceptualizar un sistema que pueda ser una herramienta útil para la auditoría de los mismos, que capacite y auxilie al auditor en el desarrollo de su actividad profesional. Es decir, que los conocimientos básicos influyen en forma directa en el soporte para la conceptualización del sistema.

I. AUDITORIA

1.- Definición de Auditoría

El término auditoría es muy antigüo y en su forma más simple implica el acto de revisar.
Revisar las cuentas que producen información financiera, así como los controles de operación y administración y la eficiencia y eficacia de los mismos dentro de una organización. De ahí que se escuchen términos como auditoría financiera, operacional o administrativa.

Pero, básicamente, ¿Qué es la auditoría?

La auditoría es una actividad profesional que técnicamente realiza el Contador Público, y consiste en la aplicación de técnicas y procedimientos a una partida o a un conjunto de controles o a un sistema de información, sometidos a revisión y evaluación, con el fin de obtener la evidencia suficiente y competente para que, a través de un juicio, se fundamente un informe u opinión, así como recomendaciones de índole práctica que resultan necesarias para el mejoramiento de la operación y control de la empresa sujeta a revisión.

Quisiera que analizáramos la definición anterior:

a) Actividad profesional... mediante la aplicación de una serie de conocimientos especializados que vienen a formar el cuerpo técnico de una actividad.

b) Básica y técnicamente realiza el Contador Público... Profesional capacitado técnicamente para la realización de un trabajo de auditoría.

c) Aplicación de técnicas y procedimientos a una partida o a un conjunto de controles o a un sistema de información, sometidos a revisión y evaluación, ... mediante la aplicación de métodos de investigación y prueba podemos cercionarnos sobre la razonabilidad de una partida o la eficacia y eficiencia de un conjunto de controles o de un sistema de información.

d) Con el fin de obtener la evidencia suficiente y competente para que, a través de un juicio, ... mediante la obtención de elementos necesarios se tengan bases suficientes para fundamentar un juicio de una manera clara y objetiva. La auditoría requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben seguirse y estimar los resultados obtenidos. Además implica que el trabajo de auditoría deberá desarrollarse cumpliendo con los lineamientos inherentes a dicha actividad.

e) Se fundamente un informe u opinión, así como recomendaciones de índole práctica que resulten necesarias para el mejoramiento de la operación y control de la empresa sujeta a revisión. El objetivo final del trabajo de auditoría será el de la preparación de un informe u opinión sobre la razonabilidad de una partida o sobre la eficiencia o eficacia de un conjunto de controles o bien de un sistema de información, como un todo, dentro de una organización.

2.- Tipos de Auditoría

Existen dos formas básicas de clasificar los tipos de auditorías:

A) Por quien la realiza.

B) Por los objetivos que se persiguen.

A) Por quien la realiza puede ser de dos formas:

a) 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.

b) Auditoría Interna: Es aquella revisión y evaluación que

realiza un auditor o grupo de auditores empleados formalmente por la organización, pero que sus funciones son ajenas totalmente a la operación de ésta. Sus actividades se limitan a las directamente relacionadas con auditoría.

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

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

b) Auditoría operacional: Su objetivo es el de evaluar totalmente el control interno de una organización, obteniendo así un informe sobre las fortalezas y debilidades del mismo.

c) Auditoría administrativa: Su objetivo es el de evaluar la eficiencia y eficacia de las operaciones de una organización para el cumplimiento adecuado de los objetivos de la misma.

3.- Fundamentos de la Auditoría.

Al efectuar un trabajo de auditoría, el auditor, adquiere responsabilidades sociales, éticas y legales ya que el resultado de su trabajo será utilizado por la empresa examinada para diferentes fines ante terceros.

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

Se clasifican en:

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

A continuación daré una explicación breve de las mismas:

a) Normas Personales

Tales normas como su mismo nombre lo indica, se refieren a las cualidades que debe reunir la persona en sí del auditor para poder dedicarse a la realización de la auditoría.

La primera de estas normas, denominada **"entrenamiento técnico y capacidad profesional"**, nos dice, hablando en términos simples, que cualquier persona que ofrezca sus servicios para el desempeño de una actividad profesional, deberá haber adquirido como base elemental el entrenamiento técnico necesario para realizar su trabajo satisfactoriamente.

En general el entrenamiento técnico, se adquiere al cumplir con los requisitos establecidos por las instituciones que ofrecen estudios conducentes a la obtención del título profesional de la carrera de Contador Público. Más no así la capacidad profesional, que se requiere, sumando a lo anterior, una madurez de juicio y una habilidad y destreza para juzgar acerca de su trabajo, que sólo lo da la experiencia profesional en el trabajo diario.

La segunda de las normas, **"cuidado y diligencia profesional"**, implica que debemos poner el mayor cuidado y diligencia profesional al realizar un trabajo de auditoría, para reducir al máximo los márgenes de error, lo que no significa ser infalible.

La tercera norma de carácter personal, **"independencia"**,

consiste en la objetividad del trabajo, esto es, que no seamos influídos en modo alguno por consideraciones de orden subjetivo.

b) Normas de Ejecución del Trabajo

La primera es la de **"planeación y supervisión"** que resulta básica ya que la planeación consiste en preveer en forma anticipada los procedimientos de auditoría que deberán ejecutarse, la extensión y la oportunidad en que serán aplicados y el personal que ha de emplearse en la auditoría.

Ahora bien, para la realización de la auditoría nos valemos de personal agrupado y jerarquizado de acuerdo al trabajo que vayan a realizar. De ahí que la delegación de trabajo es indipensable, pero la supervisión lo es aún más ya que debemos cerciorarnos de la efectividad y autenticidad del trabajo, así como de los resultados del mismo.

La segunda de las normas de ejecución del trabajo es **"estudio y evaluación del control interno"** y consiste básicamente en efectuar un estudio y evaluación adecuados de control interno existente, que sirva de base para determinar el grado de confianza en él; asimismo, que permita determinar la naturaleza, extensión y oportunidad

que va a dar a los procedimientos de auditoría.

En el capítulo"III" hablaré con más detalle acerca del control interno.

La tercera y última es **"la obtención de evidencia suficiente y competente"**, es importantísima, ya que de ésta se derivan los elementos de juicio necesarios en los que se apoya la opinión de auditoría y por consiguiente sirva de soporte a las conclusiones.

Al hablar de suficiencia, no quiere decir que se obtenga toda la evidencia posible, sino únicamente aquella que realmente sirva para justificar la opinión o informes. Y analizando el término competente, la evidencia debe circunscribirse a aquellos aspectos que tienen influencia en el juicio y la opinión.

c) Normas de Información

Estas normas son relativas al resultado final del trabajo de auditoría, es decir, al informe u opinión.

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.

II.- Auditoría de Sistemas de Información

1.- Generalidades

Los sistemas de información son el conjunto de elementos humanos, procedimientos manuales y procedimientos basados en medios electrónicos que en forma coordinada proporcionan información para la toma de decisiones en una organización. Así pues, cuando los sistemas de información se basan en computadoras (medios electrónicos) se convierten en herramientas útiles pues se aplican en los trabajos administrativos y de operación. Estos sistemas pueden ejercer control sobre muchos de los activos y las operaciones de una organización. Además el desarrollo y mantenimiento de tales sistemas pueden exigir gran parte de los recursos totales de la organización .

Debido a lo anterior y en vista de que los sistemas de información basados en computadoras se convierten en una parte integral de la operación administrativa y financiera de la organización y que además se están volviendo más extensos y complejos, surge la necesidad de diseñar técnicas especializadas de revisión de estos sistemas que permitan soportar la confianza en los mismos.

2.- Definición de Auditoría en Sistemas de Información

La Auditoría en Sistemas de Información es un concepto que ha

venido utilizándose durante los últimos años en el ámbito profesional. Deseo aportar una definición que proporcione una idea fiel de lo que es o se pretende que sea. Sin embargo, no me gustaría pasar por alto algunas definiciones de autores que lo han pretendido.

El C.P. Gustavo Adolfo Solís Montes la define como un "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 encuentren almacenados en dispositivos electromagnéticos o impresos en listados emitidos por la computadora.(1)

Ron Weber nos 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.(2)

También la Fundación de Auditores del Procesamiento Electrónico de Datos nos 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

(1) Solís Gustavo.Tesis.Introducción a la Auditoría en Informática
(2) Weber Ron.- EDP AUDITING.Conceptual Foundations and Practice

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 qué 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.

Como podemos apreciar las tres definiciones coinciden principalmente en la idea del mantenimiento de una integridad de datos adecuada para que el sistema proporcione información veraz y precisa.

Ahora bien, basándome en las definiciones anteriores presento a continuación una definición de auditoría de sistemas de información:

La auditoría de sistemas de información es una técnica aplicable a cualquier tipo de auditoría que consiste en la aplicación de procedimientos especializados dirigidos a sistemas de información automatizados para obtener la evidencia suficiente y competente a fin de evaluar y opinar acerca de si el sistema mantiene una integridad de datos, si se tienen los métodos adecuados para la salvaguarda de activos, si la información es veraz y confiable y si se apega a los objetivos organizacionales para los cuales fue diseñado el sistema.

Es importante señalar que los objetivos de la auditoría como tal no cambian a causa del sistema, lo que cambia son las herramientas y técnicas utilizadas por el auditor para alcanzar estos objetivos. Es decir, la selección adecuada de las técnicas y procedimientos de auditoría que se relacionan efectivamente con el procesamiento electrónico de datos demanda que el auditor tenga suficientes conocimientos de los componentes del ambiente computacional.

3.- Fundamentos de la Auditoría de Sistemas de Información

A la auditoría de sistemas de información le son aplicables las normas de auditoría ya comentadas en el capitulo I punto 3 (Fundamentos de Auditoría) o sea las **normas personales, de ejecución al trabajo y de información** emitidas por la Comisión de Normas y Procedimientos de Auditoría del Instituto Mexicano de Contadores Públicos A. C. . Sin embargo la Fundación de Auditores del Procesamiento Electrónico de Datos publicó en 1985 un folleto intitulado "Normas Generales para la Auditoría de Sistemas".

Estas normas son aplicables a la auditoría de sistemas de información practicada por los miembros de la Asociación de Auditoría del Procesamiento Electrónico de Datos y por los poseedores del Certificado en Auditoría de Sistemas de Información, a partir del 1º de Enero de 1988.

Quiero aclarar que la fundación y la asociación antes mencionadas regulan la Auditoría de Sistemas de Información a nivel mundial. En nuestro país la Asociación Mexicana de Auditores en Informática (AMAI) representa a México ante la Asociación de Auditoría del Procesamiento Electrónico de Datos.

Dichas normas son las siguientes:

a) Independencia

1) Actitud y Apariencia: El auditor en sistemas de información será independiente del auditado en actitud y apariencia en todo asunto relativo a la auditoría.

2) Relación Organizacional: El funcionamiento de la auditoría de sistemas de información deberá mantenerse suficientemente independiente del área bajo revisión con objeto de lograr terminar la auditoría con objetividad.

3) Código de Etica Profesional: El auditor en sistemas de información deberá apegarse a los términos del Código de Etica Profesional de la Fundación de Auditores del Procesamiento Electrónico de Datos.

b) Competencia Técnica

1) Habilidad y conocimientos: El auditor en sistemas de información deberá tener la competencia técnica adecuada y poseer las habilidades y conocimientos necesarios para el buen cumplimiento de su trabajo.

2) Estudios profesionales continuos: El auditor en sistemas de información se mantendrá al día en cuanto a competencia técnica a través de educación continua.

c) Ejecución del trabajo

1) Planeación y Supervisión: Las auditorías de sistemas de información serán planeadas durante el curso de la auditoría, evidencia comprobatoria de naturaleza y grado suficiente que le permitan apoyar debidamente los resultados y conclusiones de su informe.

2) Debido cuidado profesional: El auditor en sistemas de información deberá ejercer el debido cuidado profesional en todos los aspectos de su trabajo, incluyendo el cumplimiento de las Normas de Auditoría Aplicables.

d) Informe del auditor

1) Información sobre el alcance de la auditoría: Al preparar su informe, el auditor en sistemas de información deberá

manifestar los objetivos de la auditoría, el período de cobertura y la naturaleza y alcance del trabajo que se llevó a cabo.

2) Informe sobre resultados y conclusiones: Al preparar sus informes, el auditor en sistemas de información dará a conocer los resultados de su revisión y sus conclusiones, así como cualquier reserva o salvedad que tuviere con respecto de la auditoría.

4.- Relación entre las Normas de Auditoría y las Normas de Auditoría de Sistemas de Información

La relación que guardan ambas es muy estrecha. Podríamos decir que las segundas estan ya contenidas por las primeras. Sin embargo, las normas de auditoría de sistemas de información carecen de un punto muy importante como lo es el estudio y evaluación del control interno que debe de llevar a cabo el auditor con el propósito básico de determinar la naturaleza, alcance y oportunidad de los procedimientos de auditoría que ha de aplicar, como lo señala la norma de ejecución del trabajo de las normas de auditoría generalmente aceptadas.

Quiero señalar que las normas de auditoría tienen carácter obligatorio y son de observancia general para todos los profesionales que ejercen la auditoría.

5.- El proceso de una Auditoría de Sistemas de Información

El proceso de auditoría, en términos generales, puede dividirse en 6 fases:

1a. Definición de los objetivos de auditoría.

En esta fase el auditor deberá establecer los objetivos del trabajo en forma clara. Recordemos que de acuerdo al tipo de auditoría serán los objetivos y alcances determinados, los cuales pueden tener una orientación financiera, operacional o administrativa.

2a. Estudio preliminar.

Esta fase está enfocada al conocimiento general de la organización. El auditor deberá obtener información relevante sobre aspectos tales como:

- La empresa en general
- La organización de la empresa y la ubicación del área de sistemas de información
- Características de los equipos de cómputo y la instalación
- Objetivos generales del sistema de información
- Principales aplicaciones que afectan el sistema

3a. Estudio y evaluación del control interno de sistemas.

Esta fase estará dirigida hacia el estudio y evaluación de todas las actividades generales de Procesamiento Electrónico de Datos.

El objeto es determinar las fortalezas y debilidades del sistema. Esto se podrá lograr a través de la aplicación de las siguientes técnicas:

- Cuestionario de control interno
- Flujos de información
- Narrativos de operación
- Entrevistas con el personal
- Observación de actividades
- Inspección documental
- Recopilación de evidencia suficiente y competente
- Identificar objetivos de control y procedimientos de control

4a. Pruebas de cumplimiento.

El propósito de estas pruebas es proporcionar una certeza razonable de que los procedimientos de control interno se aplican en la forma adecuada y de acuerdo a los objetivos por los cuales fue creado. Estas son pruebas indispensables para que pueda confiarse o no en los procedimientos de control establecidos.

Por lo tanto el auditor debe dirigir sus pruebas de cumplimiento para verificar que los procedimientos de control existen, funcionan y se aplican en forma consistente.

5a. Evaluación final del control interno de sistemas.

En esta fase se concluye si el control interno de sistemas es confiable y efectivo. De tal forma que pueda el auditor fundamentar si se aplican más pruebas al control interno de sistemas o si se aplican pruebas sustantivas, es decir, pruebas para verificar las características de la información que produce el sistema basándose en la confiabilidad del control interno existente, o bien, no aplicar más pruebas en virtud de la carencia de control, lo que implicaría hacer una revisión exhaustiva.

6a. Elaborar un informe.

El proyecto final del trabajo efectuado será un informe que indique:

- Objetivo de la auditoría
- Alcances dados a la revisión
- Observaciones o deficiencias de control detectadas
- Impacto de las deficiencias
- Resultados de las pruebas efectuadas

- Sugerencias
- Conclusiones

Quiero señalar que la aplicación de estas fases estará en función de la importancia que el Procesamiento Electrónico de Datos tenga dentro de la organización examinada. Asimismo, deberán ser aplicadas en orden progresivo de tal forma que el término de una motive la ejecución de la siguiente.

III.- CONTROL INTERNO

1.- Definición y objetivos del control interno

El Instituto Mexicano de Contadores Públicos a través de la Comisión de Normas y Procedimientos de Auditoría nos dice que 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 exactitud y confiabilidad de su información financiera, promover eficiencia operacional y provocar adherencia a las políticas preescritas por la administración".

Es importante comentar que aún cuando la definición anterior tiene un enfoque de auditoría financiera al referirse a la "exactitud y confiabilidad de información financiera", el concepto es muy válido para cualquier tipo de auditoría.

Por lo que, bajo este mismo marco, debemos considerar que el control interno comprende todos los planes de organización destinados al logro de sus objetivos, asimismo, todos los métodos y procedimientos que le permiten a la misma proteger sus activos, confiar en la exactitud y veracidad de la información que ésta produce como resultado del funcionamiento eficiente y eficaz de su sistema de información y al mismo tiempo provocar la adhesión a las políticas implementadas por la administración.

Tomando como base lo anterior, podemos decir que el control interno tendrá cuatro objetivos básicos que son:

a) Salvaguarda de activos
b) Integridad de la información
c) Eficiencia operativa
d) Efectividad de las funciones

Como podemos apreciar se refieren a: información, protección, eficiencia y efectividad.

La información completa, verídica, segura y oportuna es básica para que una organización pueda tomar decisiones.

Sobre la protección, debe buscarse que los activos estén salvaguardados contra cualquier elemento negativo que pueda dañar o afectar su uso o funcionamiento.

Por último, sobre la eficiencia y eficacia podemos decir que harán una operación y administración adecuada a la organización.

2.- Elementos de Control Interno

Los elementos del control interno se constituyen de la siguiente forma:

a) Organización:

a.1) Dirección: Este elemento representa la función de dirigir todos los recursos de una organización hacia el logro de los objetivos organizacionales.

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.

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.

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.

b) Procedimientos

b.1) Planeación y Sistematización: Debe existir una planeación adecuada de activivdades 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.

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.

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.

c) Personal

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

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

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.

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.

d) Supervisión:

Este último elemento de control interno representa un agente de control dentro 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.

3.- Relación del Control Interno con el Auditor

El auditor lo evalúa no únicamente como un requisito preestablecido, sino como un elemento necesario para el desarrollo de su trabajo, ya que mediante la revisión del control interno el auditor puede obtener una imagen de la organización y de los procedimientos que la empresa tiene establecidos para el logro de sus objetivos, consecuentemente, el auditor una vez evaluado el control interno, tendrá elementos de juicio suficientes en calidad y en cantidad para determinar las pruebas que desea realizar para verificar el cumplimiento de objetivos, cualquiera que estos sean.

Los aspectos relacionados con las pruebas de auditoría que el auditor puede determinar con base a los resultados del estudio y evaluación del control interno son los siguientes:

- Naturaleza: Esta característica representa el tipo de prueba que el auditor debe realizar, es decir, el COMO.

- Alcance: Esta característica representa que proporción del universo deberá revisar el auditor, es decir, el CUANTO. En muchas ocasiones, el auditor se auxilia de métodos de muestreo incluyendo el método estadístico.

- Oportunidad: Esta característica representa el tiempo en que se deberá aplicar la prueba de auditoría, es decir, el CUANDO.

4.- 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 consisten 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. Ejemplos de ellos son: cifras control, passwords, conciliación de cifras, etc.

- Correctivos: Estos procedimientos tienen 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. Un ejemplo sería 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. Un ejemplo sería un procedimiento de conciliación de cifras control.

5.- Impacto del Proceso Electrónico de Datos en el Control Interno

El uso de equipo de procesamiento electrónico de datos no impacta los objetivos de control interno, sin embargo, si existe un impacto en sus elementos, el cual se refleja en una adecuación de los

mismos.

El empleo de tecnologías de procesamiento electrónico de datos ha proporcionado a las empresas grandes ventajas sobre el manejo de elevados volúmenes de información y en reducción del tiempo requerido para los procesos. Sin embargo, ésta relativamente nueva y cambiante tecnología también ha propiciado un alto nivel de dependencia hacia las computadoras, pues como lo menciona Ron Weber en su libro EDP Auditing, Conceptual Foundations and Practice: "existe un gran número de empresas que su supervivencia sin computador se ve reducida a unos cuantos días e inclusive a horas".

Como cualquier otro elemento de alta tecnología que implique un cambio en la cultura organizacional de las empresas, el empleo del procesamiento electrónico de datos representa nuevos riesgos tales como:

- Segregación de funciones:

  El uso del PED no únicamente modifica la segregación de funciones tradicional de las empresas (separación de funciones de inicio, autorización, ejecución y registro de transacciones), sino que genera nuevas funciones que deben observar una adecuada segregación.

- Tecnología cambiante:

  Casi ninguna área tecnológica posee un nivel de cambio tan alto como la tecnología de computación, lo cual puede traer consecuencias para la organización, desde aspectos motivacionales al personal de sistemas, hasta aspectos de competitividad en el mercado.

- Concentración de Información (custodia):

  El empleo de equipos de procesamiento electrónico de datos implica que toda la información de la organización se almacene en un solo lugar.

- Concentración de Control:

  Principalmente al iniciarse en el empleo de equipos computacionales, las organizaciones muestran una tendencia de concentración de control en el área de sistemas, funciones que muchas veces rompen el esquema de una adecuada segregación de funciones entre los departamentos usuarios y el área de informática.

6.- Necesidad de Control en Computación

En los sistemas manuales los controles se efectuaban por una

persona revisando el trabajo de otro. En la actualidad con el uso o empleo de sistemas de información automatizados la computadora realiza casi cualquier trabajo de procesamiento de datos con poca o casi nada de intervención humana. Además toda la información del sistema está en manos de un número reducido de personas que se comunica directamente con la computadora. Por eso la organización deberá tener los controles necesarios para evitar que exista:

a) Costo por pérdida o mal uso de la información

   Ejemplificado por la posible pérdida de los registros de cuentas por cobrar en una empresa comercializadora o el traspaso ilícito de un archivo maestro de clientes a un competidor.

b) Decisiones erróneas

   Uno de los mayores problemas que existen en la actualidad es la toma de decisiones erróneas basadas en sistemas de información también erróneos. Algunos autores consideran que es peor contar con información equivocada o inexacta para la toma de decisiones a no contar con ninguna información en absoluto.

c) Información: oportuna y correcta

Dos de las características más importantes en la información son su oportunidad y su corrección. El contar con o carecer de información correcta en un momento determinado tendrá su efecto en la toma de decisiones, asimismo en algunos casos representa recursos económicos que afectan directamente a la organización.

d) Falta de capacitación del personal del área de sistemas

Muchas veces la falta de capacitación adecuada en el personal del área de sistemas no sólo ocasiona el desperdicio de recursos al no utilizar eficientemente el equipo, sino que puede llegar en algunos casos a propiciar errores costosos para la empresa; aún cuando las computadoras son muy confiables en cuanto a lo que hacen, éstas sólo realizan aquello para lo que se les programa y únicamente con la información que les proporciona el ser humano, y bajo su manejo los errores en éste aspecto pueden ser el origen de pérdidas cuantiosas.

e) Manipulación de la Información

La posibilidad que tiene un programador de manipular a un computador es muy elevada. Un programador no necesita tener acceso directo al equipo de computación para obtener el control de grandes cantidades de activos,

omitiendo programas con rutinas sutilmente intercaladas para perpetrar un fraude o evadir los controles existentes.

f) Falla de los equipos

Debido al acelerado ritmo de trabajo con que se utilizan los equipos de cómputo las fallas en los mismos constituyen un riesgo potencial para la información que se procesa.

g) Vandalismos y catástrofes naturales

Estos últimos aunque menos probables no dejan de representar amenazas para la instalación.

h) Fraude vs. Error o Negligencia

Fraude involucra dolo y premeditación en un acto que perjudica a la empresa en donde se efectúa; el error o negligencia son simplemente dos características que acompañan eternamente al ser humano.

7.- 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 de 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

Los controles generales son los procedimientos de control interno adoptados en una instalación de cómputo que tienen impacto en todos los sistemas de información , es decir, se enfocan a la organización general del área de Procesamiento Electrónico de Datos y a las funciones de quienes intervienen en el desarrollo de sistemas; esto es, el medio ambiente en que se desarrollan los sistemas.

Estos controles se dividen en las siguientes áreas de controles generales:

- Organización del área de sistemas
- Administración de los recursos informáticos
- Desarrollo y mantenimiento de Sistemas
- Operación de centros de cómputo

- Sistema operativo y software de base de datos
- Seguridad física y lógica

b) Controles de aplicación

Los controles de aplicación que se refieren a los establecidos en la operación del computador que incluye la entrada, el proceso y salida de datos. Podríamos decir que son procedimientos de control aplicados a un sistema de información como puede ser un sistema de nómina o inventario. Son controles que se establecen para la operación del sistema, y se dividen en las siguientes áreas de aplicación:

- Identificación, preparación y captura
- Entrada de datos
- Acceso a la información
- Comunicación de datos
- Proceso de datos
- Salida y distribución
- Respaldo y recuperación
- Documentación

Es necesario decir que por el Procesamiento Electrónico de Datos de suma importancia en el manejo de información, el auditor deberá contar con las herramientas suficientes que le permitan estudiar y evaluar el control interno.

IV.- Controles Generales.

1.- Generalidades

Para que los resultados que se obtienen en un sistema de procesamiento electrónico de datos sean confiables, es necesario implantar una serie de controles.

Los controles generales son los procedimientos de control interno adoptados en una instalación de cómputo que tienen impacto en todos los sistemas de información. Dicho en otros términos, se enfocan a la organización general del área de sistemas.

Los controles generales se aplican uniformemente a todos los sistemas de información automatizados de la organización. Por lo que podemos decir que son globales sobre cada aplicación que se procesa en el sistema y afectarán las fortalezas, debilidades y confianza de ésta.

2.- Areas de controles generales

Aún cuando el número de controles que se pueden establecer es muy grande y, en la práctica , existen diferencias de consideración de una instalación a otra, podemos dividir a los controles generales en las siguientes áreas:

2.1.- Controles de organización

Con el uso de sistemas de información automatizados las fuentes y recursos de información tienden a centralizarse. La centralización trae consigo grandes oportunidades de error e irregularidades.

Una de las maneras o formas de eliminar esta vulnerabilidad es a través de controles que proporcionen una estructura organizacional.

Un plan organizacional coherente puede ayudar a componer la pérdida de control, dividiendo las tareas entre distintas personas o mediante la segregación de funciones.

Cuatro elementos pueden ser identificados en los controles organizacionales:

a) Segregación de funciones

Para un control efectivo deberá existir separación entre el área de procesamiento electrónico de datos y el departamento que origina o usa información del sistema.

b) Asignación de responsabilidades

Implica que las tareas de trabajo y las secuencias deberán ser estructuradas de manera que todas las tareas sean asignadas con responsabilidades específicas.

c) Rotación de deberes

La asignación de trabajo puede ser variado para asegurar que ninguna persona esté expuesta repetidamente a una aplicación que pueda motivar aburrimiento o una intromisión con el sistema.

d) Supervisión

Este es un elemento indispensable que consiste básicamente en la observación, autorización y aprobación de las actividades realizadas por otra persona.

Basados en lo anterior podemos definir los objetivos del control organizacional y los procedimientos mínimos de control del mismo:

Objetivos del control:

1.- Objetivos del sistema acordes a los objetivos de la organización.
2.- Adecuada segregación de funciones y asignación de responsabilidades.

3.- Adecuada supervisión de actividades.

4.- Adecuada planeación a corto y largo plazo que asegure un correcto y continuo funcionamiento del área de sistemas.

Procedimientos de control:

1.- Existencia de un organigrama formal del área de procesamiento electrónico de datos.

2.- El área de procesamiento electrónico de datos reporta a un nivel más alto al de sus usuarios.

3.- Existencia de definición de puestos y descripción de funciones.

4.- Definición de la división de funciones:

Area de sistemas - Usuario

Programación - Operación

Control - Operación

Control - Programación

Cintoteca - Operación

2.2.- Administración de los recursos

Una adecuada administración del área de procesamiento electrónico de datos es importante ya que facilita un desarrollo exitoso y continuo en la implantación de sistemas de información.

Elementos como la planeación, que permite asegurar una adecuada adquisición de equipo y su implantación a través de planes de factibilidad e implantación o la selección adecuada de personal de sistemas, que permite que se seleccione al más idóneo de acuerdo a los requerimientos de trabajo del área, o al desarrollo y capacitación de personal que asegura promociones adecuadas, oportunidades de crecimiento del personal y el adecuado manejo de los recursos de sistemas de información y por último el establecimiento de estándares que aseguran control de actividades, análisis y diseño de sistemas así como su mantenimiento, hacen de los controles de administración una parte importante y fundamental del área de procesamiento electrónico de datos ya que depende de estos el éxito o el fracaso de los sistemas de información en una organización.

Los objetivos del control de administración son los siguientes:

1.- Adecuada adquisición de equipos de cómputo acorde a los objetivos y planes de la organización.

2.- Adecuada utilización de los recursos de sistemas en la consecución de objetivos y planes de la organización.

3.- Adecuada estandarización de procedimientos administrativos y de sistemas que implica que los sistemas son utilizados correctamente.

4.- Eficiente utilización de los recursos de sistemas.

Los procedimientos de control a través de los cuales se pueden asegurar los objetivos de control antes mencionados son:

1.- Existe una metodología y estudios de viabilidad y selección de equipo.
2.- Establecimiento de un comité de usuarios formal.
3.- Elaboración de un manual de políticas y procedimientos.
4.- Existe un plan de sistemas a corto y largo plazo.
5.- Existen planes de capacitación para el personal.
6.- Adecuado control presupuestal del área.
7.- Adecuado tratamiento de costos y gastos del área.
8.- Supervisión adecuada para el área.

2.3.- Controles de Desarrollo y Mantenimiento de Sistemas

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 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 objetivos de los controles de desarrollo y mantenimiento de

sistemas pueden ser para:

1.- Que una aplicación se convierta al computador cuando ello genere mayores beneficios que cualquier otra alternativa.
2.- Los sistemas se desarrollan en forma eficiente y satisfacer los objetivos para los cuales se crean.
3.- Los sistemas sean modificados única y exclusivamente cuando sea justificado y bajo los mismos controles que se aplicaron en su desarrollo.
4.- Todos los sistemas contarán con documentación suficiente y actualizada que permita realizar las funciones de mantenimiento, operación y proceso en forma efectiva y eficiente.

Los procedimientos de control de desarrollo y mantenimiento estarán enfocados a asegurar:

1.- La existencia de estándares para las funciones de:

a) Desarrollo de sistemas:

- Análisis y Diseño de sistemas
- Programación
- Prueba de sistemas
- Implantación de sistemas

- Documentación
- Capacitación de usuarios
- Seguimiento y post-evaluación

b) Mantenimiento de Sistemas

- Solicitud, evaluación y autorización de modificaciones
- Procedimientos de modificación de los sistemas
- Procedimientos de prueba de las modificaciones
- Autorización de cambios
- Documentación de modificaciones

2.- Que el usuario participe en el análisis de aplicaciones

3.- Que se ejerce control de tiempos y recursos

4.- Los operadores no ejercen funciones de programación

2.4.- Controles de Operación de Centros de Cómputo

Estos controles estan 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 de operación pueden ser entre otros:

1.- Que el centro de cómputo se utilizará para el proceso de información en forma eficiente

2.- Que el centro de cómputo contará con procedimientos para prevenir y/o detectar errores e irregularidades en el proceso de datos

3.- Que el centro de cómputo proveerá los recursos necesarios para asegurar la continuidad e integridad del proceso de información

4.- Que la configuración del equipo de cómputo debe ser acorde a la organización de la empresa

Ahora bien, los procedimientos de control que de acuerdo o tomando como base lo anterior deberán asegurar que:

1.- Existe un calendario de producción

2.- Los trabajos procesados se supervisan

3.- Existen procedimientos para la asignación de prioridades

4.- Existe una bitácora de trabajos procesados

5.- Las bitácoras son supervisadas y comparadas contra los calendarios de producción

6.- Los operadores no tienen acceso a archivos en producción

7.- No se efectuan correcciones a documentos fuente

8.- Los programadores no operan el equipo

9.- Existe una función de bibliotecario independiente a

operación

10.- Los discos, cintas y diskettes cuentan con etiquetas exteriores de identificación

11.- Existe un control de fallas y registro de mantenimiento correctivo

12.- Existe un calendario de mantenimiento preventivo

13.- Existen instalaciones alternas para soporte de proceso

14.- Existe rotación de turnos

15.- Existen estándares para los operadores sobre:

- Errores de hardware
- Errores de software
- Errores de aplicaciones
- Errores en instalaciones

2.5.- Controles del Sistema Operativo y Base de Datos

Estos controles estarán dirigidos a la salvaguarda y buen uso del software de los sistemas de información automatizados. Por tal motivo los objetivos de control que persiguen son:

1.- Que el software de la instalación representa la opción más adecuada de acuerdo a las propias características de la instalación y de los objetivos de la organización

2.- Que el software de la instalación cuenta con documentación suficiente y actualizada

3.- Que la integridad del software de la instalación se

encuentra debidamente garantizado

Los procedimientos de control para los objetivos antes mencionados deberán asegurar que:

1.- Existen responsables de software del sistema y sus funciones son independientes de otras áreas de Procesamiento Electrónico de Datos y de los usuarios
2.- Existen funciones definidas
3.- Se cuenta con documentación de software
4.- El acceso al software esta limitado al personal autorizado
5.- La organización de la base de datos es adecuada a las características operativas de la empresa
6.- Existen estándares para el mantenimiento al software de la instalación

2.6.- Controles de Seguridad Física y Lógica

Estos controles deben incluir todas las operaciones físicas y de procedimiento utilizadas para asegurar que el sistema de información no será interrumpido (intencionalmente o no) por fuerzas internas o externas.
Asimismo, deberá proporcionar al sistema seguridad en los accesos al mismo.

Los objetivos de control serán, entre otros:

1.- El equipo e instalaciones de cómputo se encuentran debidamente protegidos contra daño, pérdida o mal uso
2.- La información almacenada en dispositivos electromagnéticos, impresa en reportes, microfilmada o transmitida a sitios remotos se encuentra debidamente protegida contro pérdida, divulgación, modificación o mal uso
3.- El software de aplicación se encuentra debidamente protegido contra destrucción, modificación o divulgación

Los procedimientos de control deberán asegurar que:

1.- Las instalaciones de cómputo no están en lugares públicos
2.- Las instalaciones de Procesamiento Electrónico de Datos son independientes arquitectónicamente de otras áreas de la organización
3.- El acceso al área de Procesamiento Electrónico de Datos y al Centro de Cómputo es restringida
4.- Existe equipo de detección y extinción de humo y fuego
5.- No existe riesgo de inundaciones
6.- El equipo de aire acondicionado funciona adecuadamente
7.- No existe material inflamable en el centro de cómputo

8.- Existe un plan de contingencias para el departamento de Procesamiento Electrónico de Datos

9.- Existe una póliza de seguros adecuada

10.- Existe un convenio de soporte con una instalación alterna

11.- Existe equipo No Break (UPS)

12.- Existen respaldos del material magnético fuera de las instalaciones de cómputo:

- Archivos
- Programas
- Sistema operativo
- Software de base de datos

13.- Existe respaldo de la documentación fuera de las instalaciones de cómputo

14.- Los programas fuente y objeto en producción se encuentran en áreas independientes

15.- Existen áreas exclusivas para desarrollo, mantenimiento y prueba de programas (preferiblemente en tres áreas independientes entre sí)

16.- Existe una biblioteca exclusiva para el sistema operativo de la instalación

17.- Existen archivos o segmentos de archivos que se utilizan para la prueba de los programas en desarrollo o mantenimiento

18.- Los programadores sólo tienen acceso a los programas en desarrollo y/o mantenimiento y a modificar los

archivos de prueba.

19.- Los operadores sólo tienen acceso a los archivos en producción mediante la ejecución de programas catalogados.

20.- Los operadores solo pueden ejecutar los programas en producción más no modificarlos o reproducirlos.

21.- El uso de compiladores y utilerías se encuentra debidamente protegido.

22.- El acceso al sistema operativo se encuentra debidamente controlado.

23.- Existe un sistema de passwords de acceso al sistema.

24.- Existen políticas y procedimientos sobre la asignación y mantenimiento de passwords.

25.- Los intentos de acceso no autorizado son detectados, reportados e investigados.

26.- Existe un adecuado control físico sobre la entrada y salida de dispositivos electromagnéticos.

3.- Auditando Controles Generales

La auditoría de los controles generales se encuentra ubicada en la tercera fase de una auditoría de sistemas de información y se conoce cón el nombre de estudio y evaluación del control interno.

Recordemos que los controles generales se aplican a todos los procesos en forma global que se llevan a cabo en una área de

Procesamiento Electrónico de Datos.

La auditoría de controles generales se puede llevar a cabo siguiendo los pasos que a continuación se comentan:

1º Realizar un repaso preliminar de controles generales

El objetivo de este paso será el de reunir suficientes antecedentes para conducir apropiadamente la revisión. Es decir, identificar los procedimientos de control que la organización auditada debería tener de acuerdo a sus características.

2º Documentar los controles generales

El objetivo de este paso es el de adquirir información tomando en cuenta los controles generales. Es decir, se deberá obtener conocimiento sobre los procedimientos de control identificados. Esto se puede hacer empleando la técnica de cuestionarios. (Véase Anexo I)

3º Probar los controles generales

El objetivo de este paso es determinar si los controles existentes están funcionando efectivamente.
Esto se logra aplicando procedimientos de auditoría.

(Véase Anexo II)

4º Evaluar la eficacia de los controles generales

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

Recordemos que el auditor esta evaluando el control interno y que de los resultados de éste será el alcance, naturaleza y oportunidad de los procedimientos de auditoría a efectuar en la siguiente fase de la auditoría de sistemas de información.

En relación a lo anterior, existe un axioma que se debe tener presente durante el desarrollo de la auditoría:

"La existencia de un adecuado nivel en los controles generales no asegura la eficiencia de los controles de aplicación; sin embargo, cuando los controles generales sean deficientes indudablemente se verán afectados los controles de aplicación". (1)

(1)Solís Gustavo.Tesis.Introducción a la Auditoría en Informática

V CONCEPTUALIZACION DEL SISTEMA PARA LA EVALUACION DE CONTROLES GENERALES

1.- Justificación

Los sistemas de información se han convertido en parte integral de la operación administrativa y financiera de la organización, además se estan volviendo más extensos y complejos.

Esto crea la necesidad de capacitación y desarrollo para la revisión de sistemas de información automatizados que le permita al auditor llevar a cabo revisiones de calidad profesional.

Lo anterior implica tiempo y costo.

El sistema puede ayudar a ahorrar tiempo y costo de una capacitación para el desarrollo de este tipo de auditorías. Por la sencilla razón de que le podrá proporcionar la ayuda necesaria para que el auditor, sin mucha experiencia en el área, pueda desarrollar satisfactoriamente su trabajo. Y al mismo tiempo le proporcionará una capacitación profesional en el área de auditoría de sistemas de información.

Quiero aclarar que el sistema no pretende ser una solución total a los problemas de capacitación que hay en el área de auditoría de sistemas, es tan sólo una herramienta de apoyo.

2.- Objetivo

El sistema para la evaluación de controles generales para el área de procesamiento electrónico de datos fue pensado para proporcionar al auditor en informática:

- una herramienta de trabajo que le permita evaluar los controles generales del área,

- medir el impacto de las deficiencias o desviaciones del área para la auditoría, tomando en consideración que se capta, procesa y se produce información,

- determinar los riesgos para el auditor en la emisión de su informe u opinión, y

- poder sugerir medidas correctivas de control para el área.

3.- Metodología del Análisis

El proceso de análisis de sistemas consiste en comprender situaciones, evaluarlas y si es preciso proponer alternativas de solución con el fin de mejorar un sistema o crear uno nuevo. Los sistemas contienen muchos componentes. Se debe investigar empezando con aspectos generales en relación con el propósito del sistema.

Existen varias estrategias para aplicar una metodología de análisis de sistemas y así determinar los requerimientos de información, una de ellas y que es la que vamos a utilizar para nuestro análisis del sistema es el análisis estructurado propuesto por Edward Yourdon en su libro "Managing The System Life Cycle".

El análisis estrucurado permitirá estudiar la forma en que se manejan los datos en cada actividad a través del seguimiento de los datos dentro de los procesos y podremos observar detalles importantes de las operaciones por medio de los diagramas de flujos de datos.

3.1 Diagramas de Flujos de Datos

Los diagramas de flujo de datos muestran gráficamente los componentes que intervienen dentro de un procedimiento específico y tienen como finalidad auxiliar a estudiarlo. Puede resultar díficil entender por completo una actividad dentro de una organización a través de una descripción. Los diagramas de flujo de datos ayudan a mostrar las partes importantes de un proceso y la forma en que interactúan.

3.2 Notación

Los diagramas de flujo de datos se pueden elaborar

utilizando cuatro símbolos:

- Flujo de datos. Movimiento de datos en una dirección específica, de un origen a un destino. Líneas con indicación de dirección de información.

- Procesos. Representa los procesos realizados por personas o dispositivos para producir o transformar datos. Circulos.

- Fuente y destino de los datos. Las fuentes y destino de los datos externos pueden interactuar con el sistema pero no son parte de él.

- Almacenamiento de datos. Aquí se almacenan o consultan datos del proceso del sistema. Puede representar dispositivos computarizados o no computarizados.

3.3 Ventajas del Método

Las notaciones descritas son sencillas.

Los usuarios pueden examinar los diagramas y señalar los problemas rápidamente de manera que pueden corregirse antes que se inicie el trabajo de diseño.

4.- ESPECIFICACION ESTRUCTURADA

DIAGRAMA DE CONTEXTO

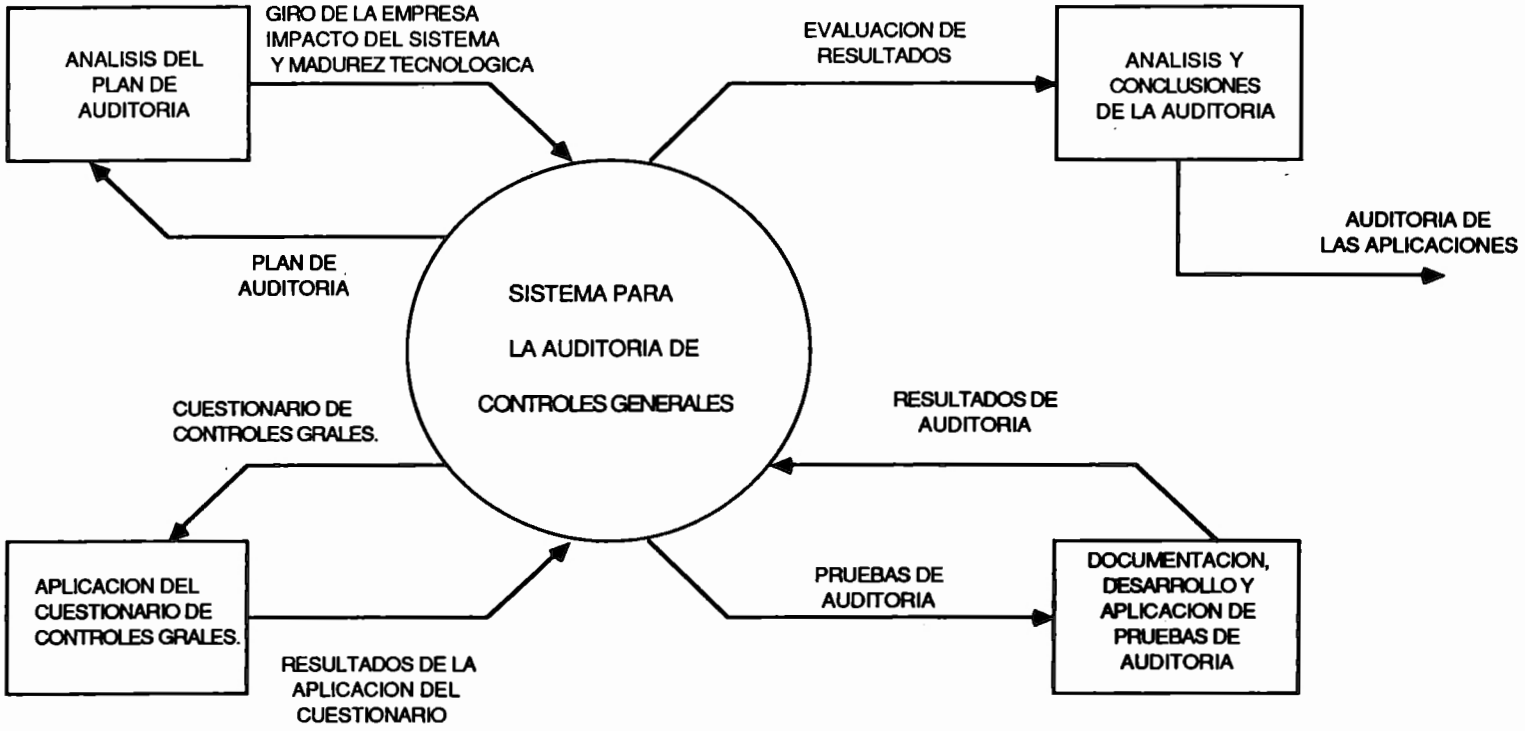


DIAGRAMA DE FLUJO DE DATOS
NIVEL CERO

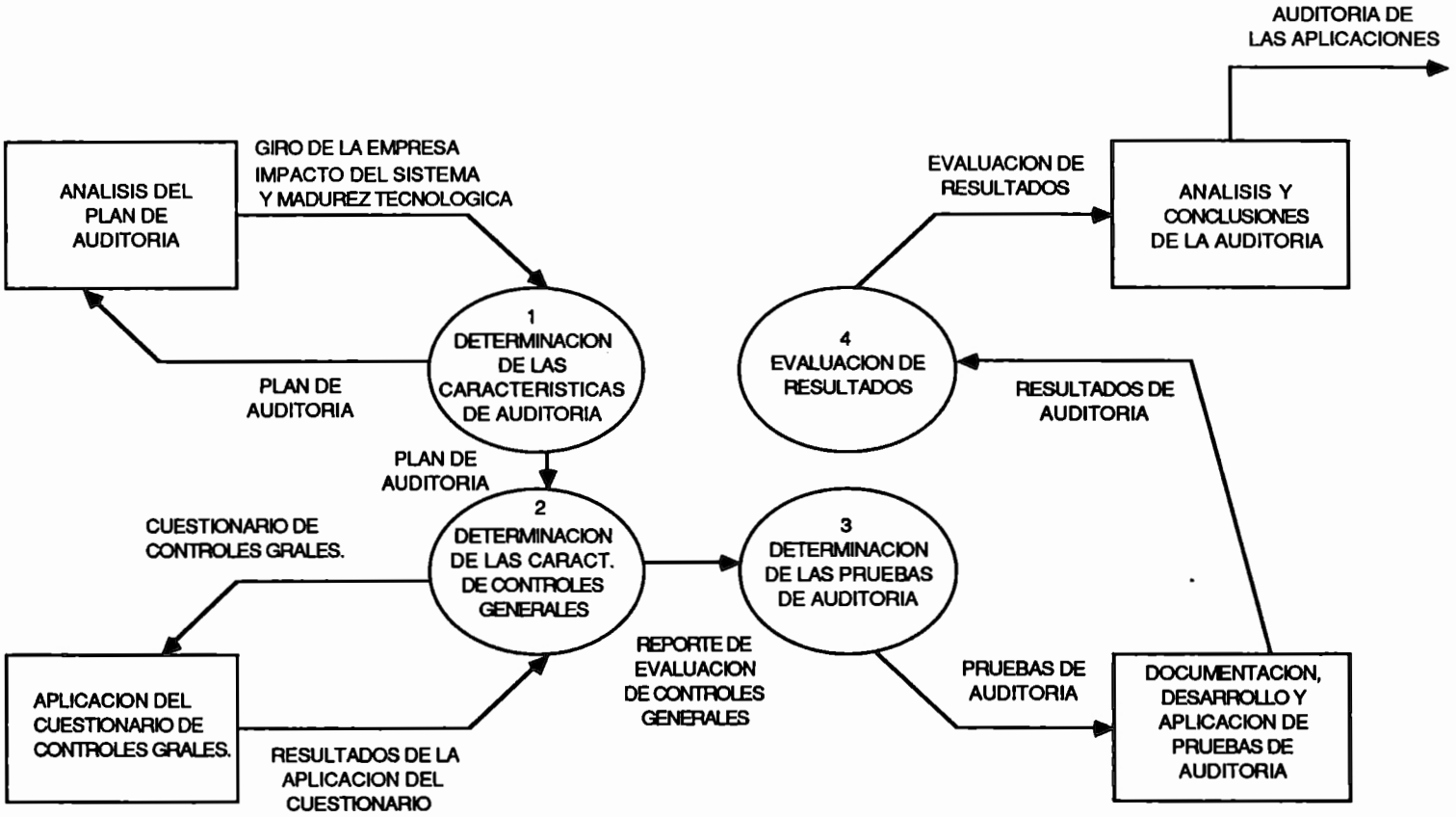


DIAGRAMA DE FLUJO
PROCESO 1 NIVEL (1)

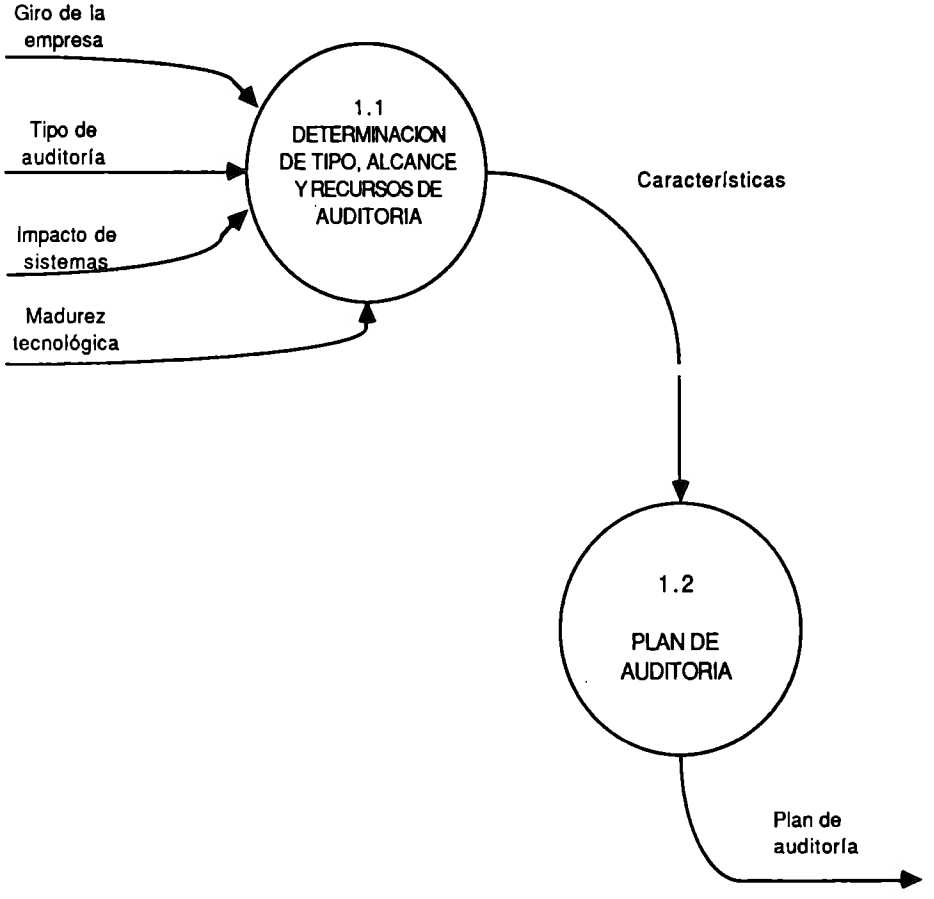


DIAGRAMA DE FLUJO
PROCESO 1.1 NIVEL(2)

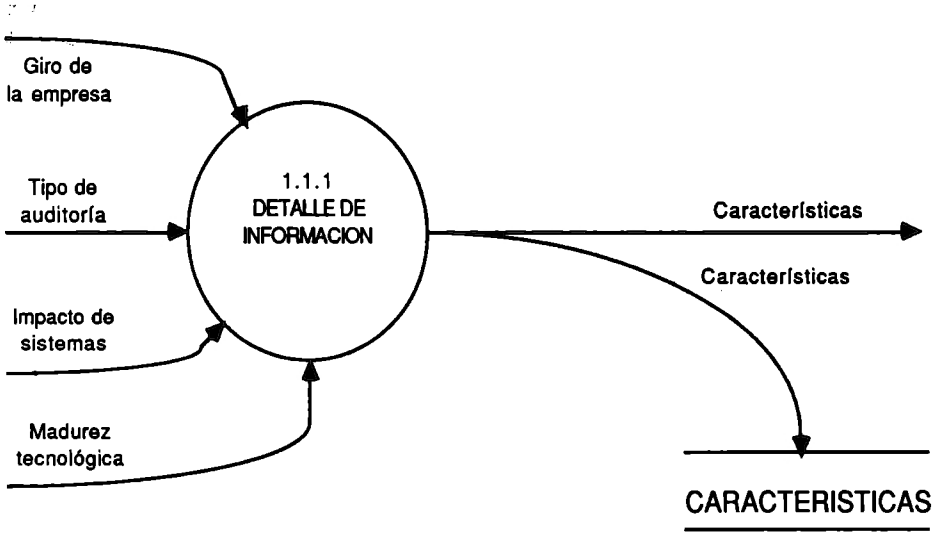


DIAGRAMA DE FLUJO
PROCESO 1.2 NIVEL (2)

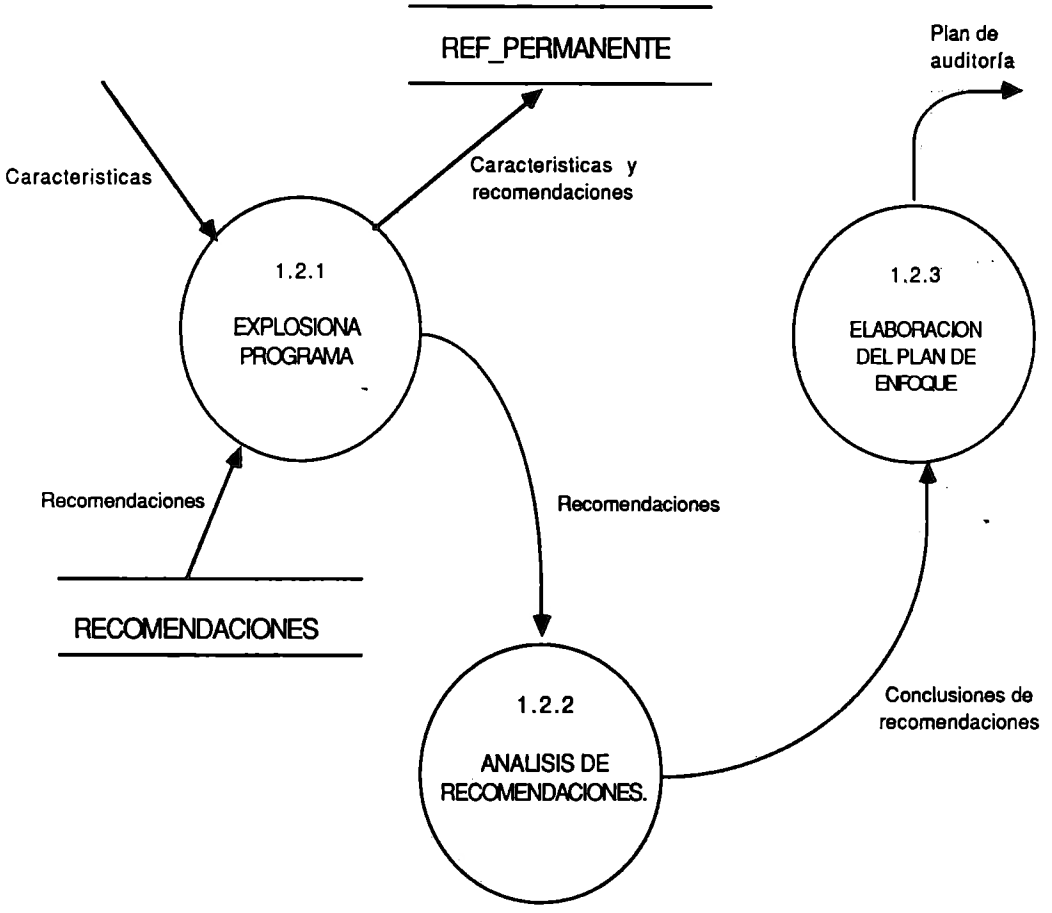


DIAGRAMA DE FLUJO
PROCESO 2 NIVEL (1)

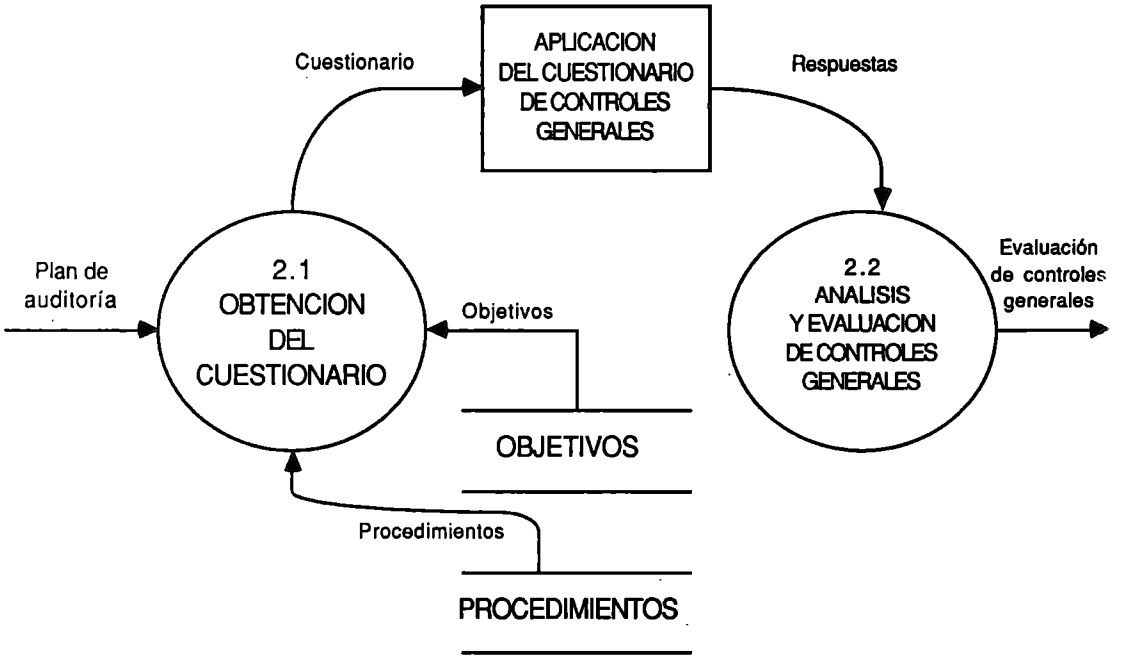


DIAGRAMA DE FLUJO
PROCESO 2.1 NIVEL (2)

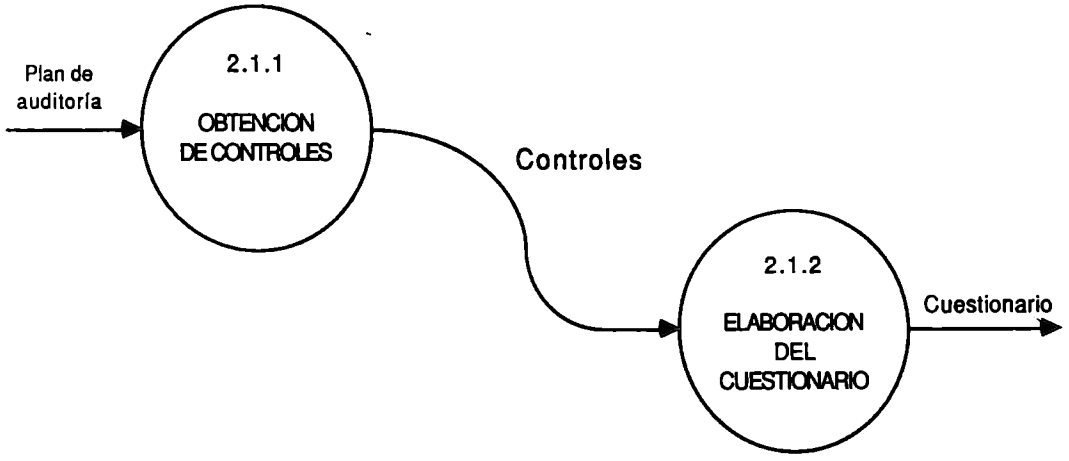


DIAGRAMA DE FLUJO
PROCESO 2.1.1 NIVEL (3)

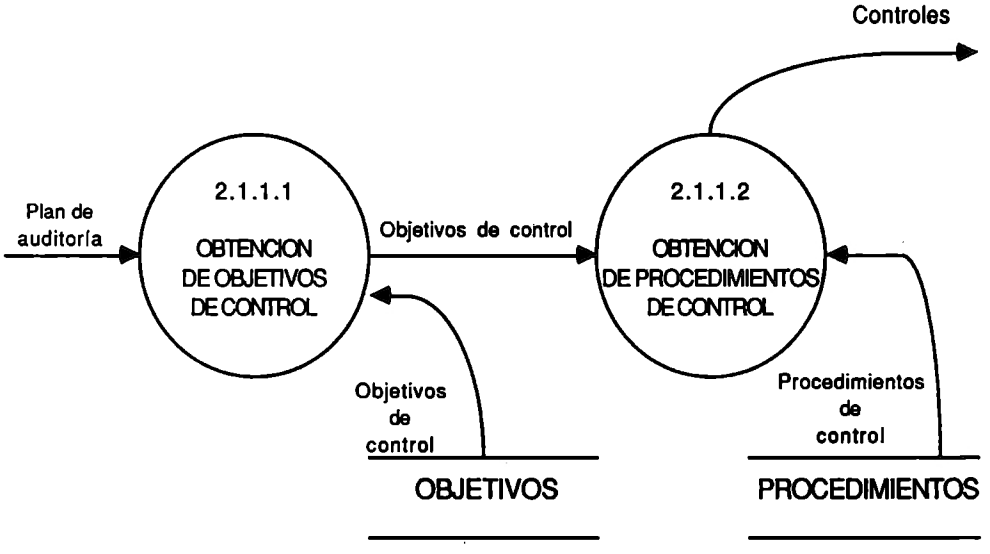


DIAGRAMA DE FLUJO
PROCESO 2.1.2 NIVEL (3)

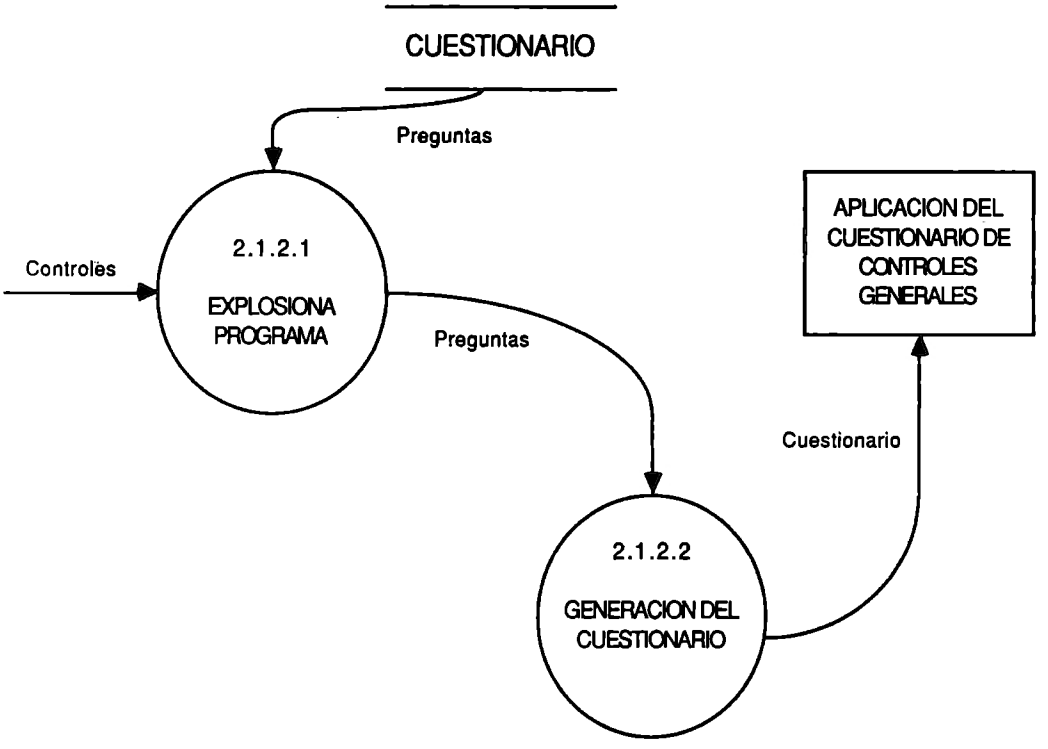


DIAGRAMA DE FLUJO
PROCESO 2.2 NIVEL (2)

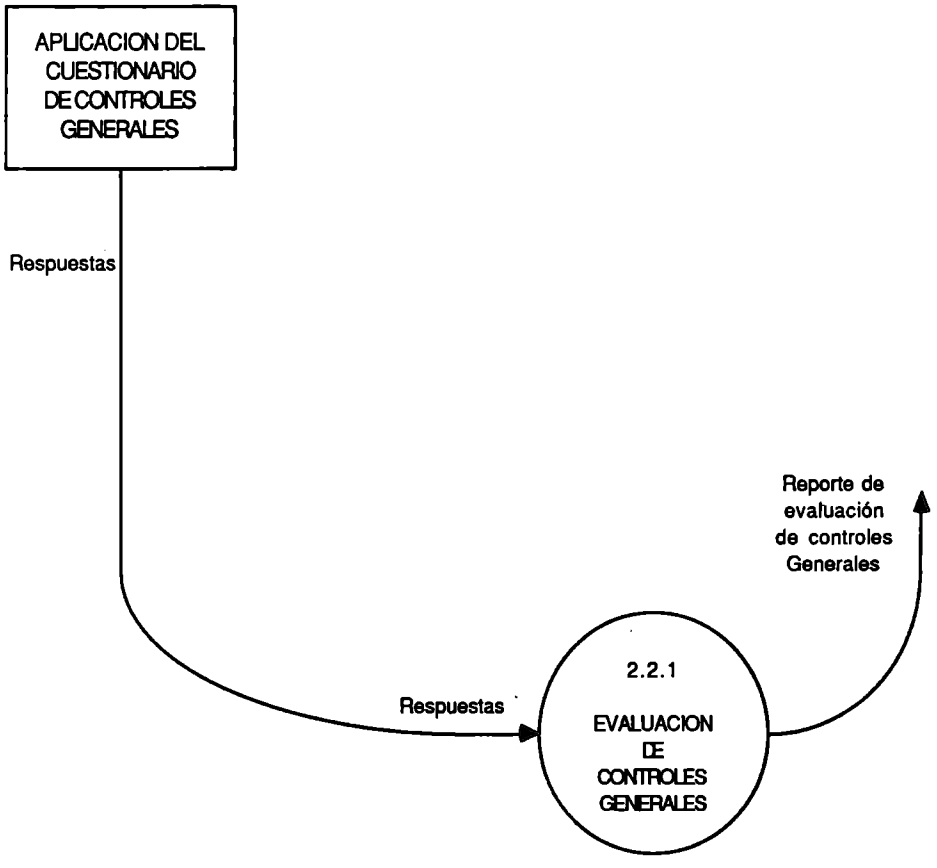


DIAGRAMA DE FLUJO
PROCESO 2.2.1 NIVEL (3)

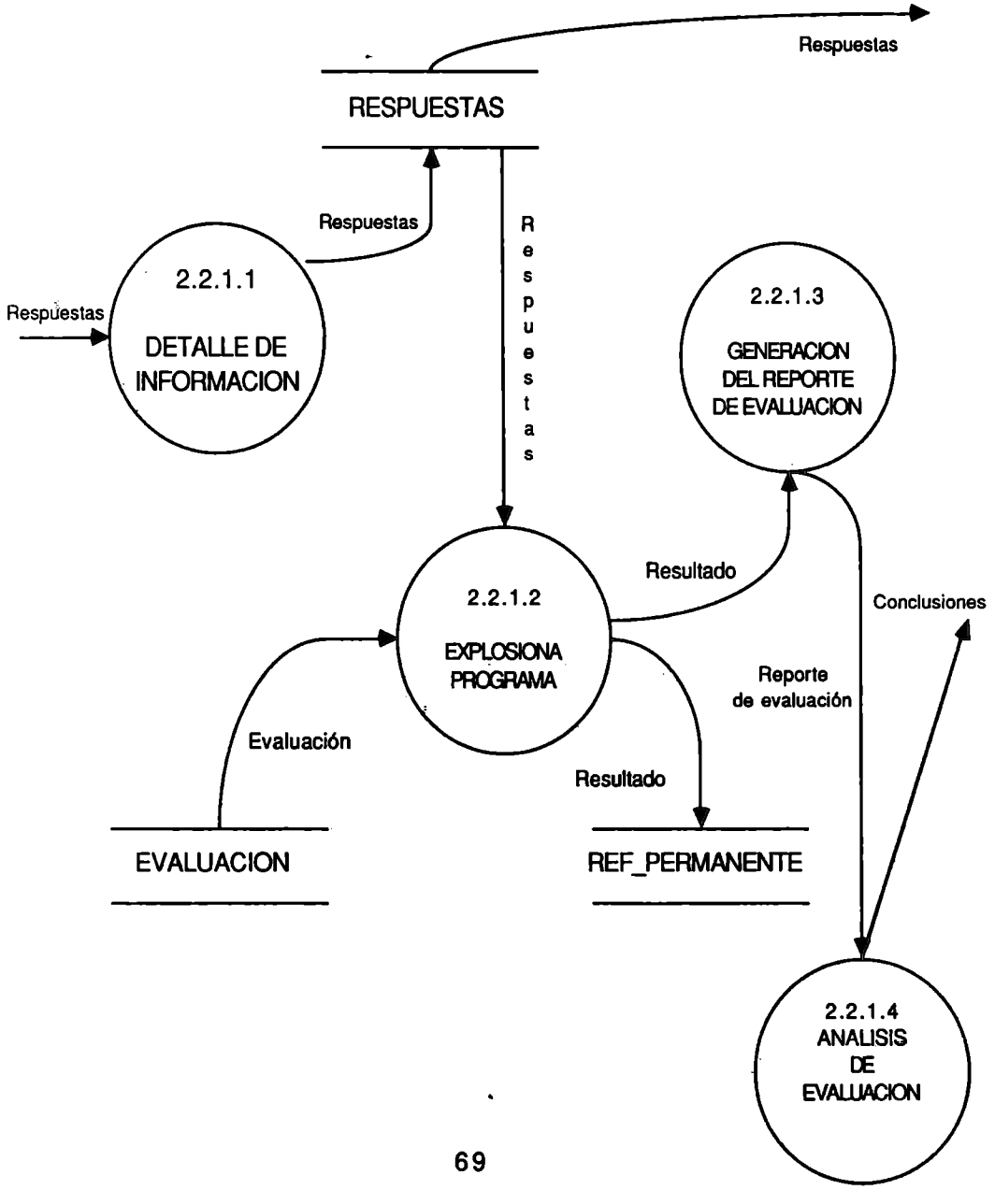


DIAGRAMA DE FLUJO
PROCESO 3 NIVEL (1)

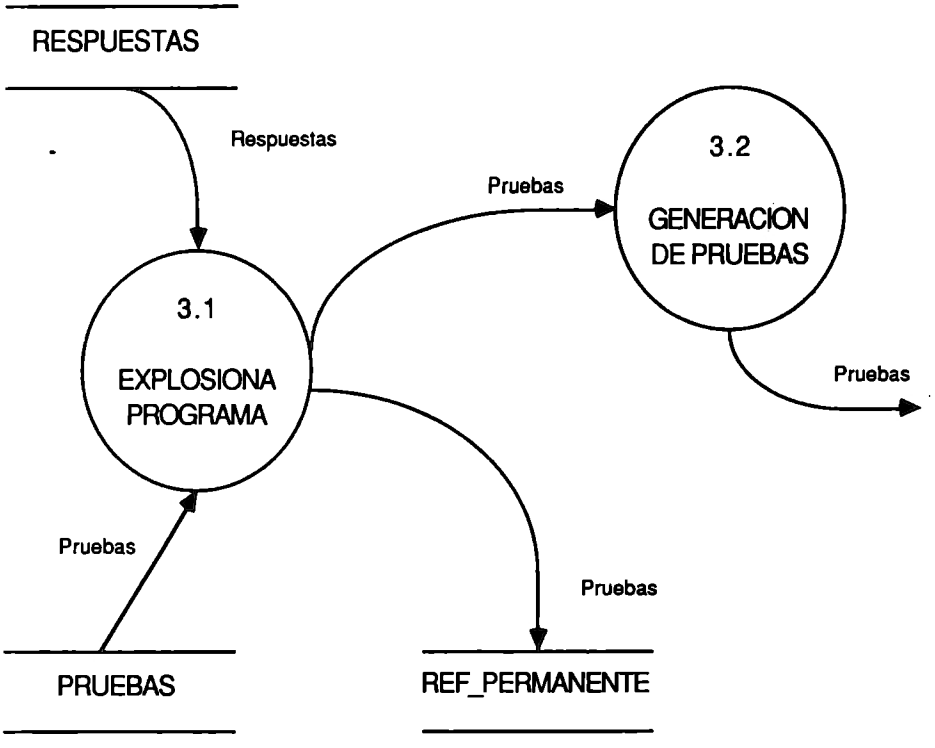


DIAGRAMA DE FLUJO DE DATOS
PROCESO 4 NIVEL (1)

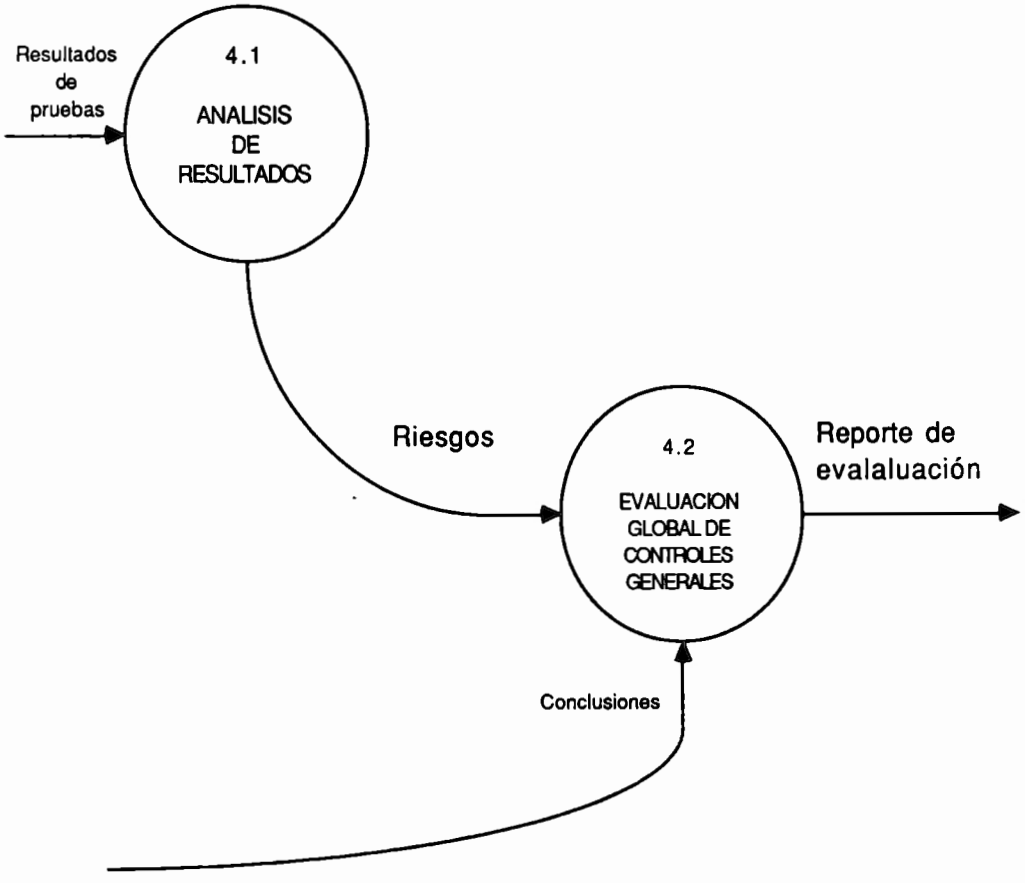
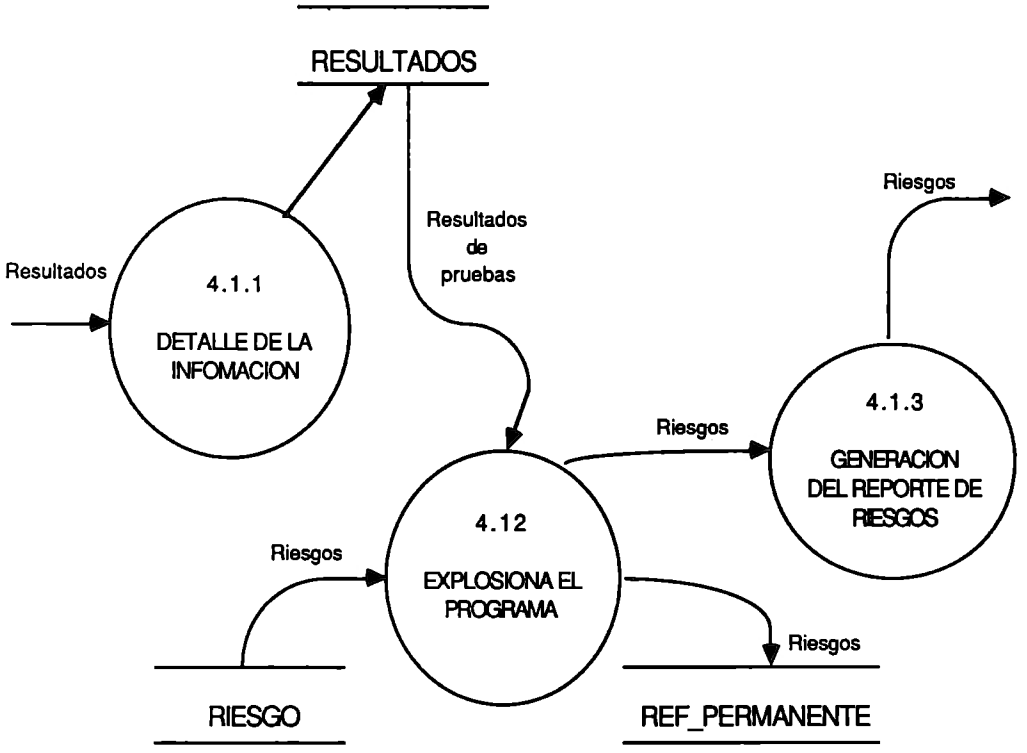


DIAGRAMA DE FLUJO DE DATOS
PROCESO 4.1 (NIVEL DOS)



4.3 Diccionario de Datos

Actividades: Detalle de las actividades que sufren paro o falla por falta de sistemas computarizados.

Aplicaciones: Número de aplicaciones que tiene el sistema.

Areas: Areas de control a evaluar por la auditoría.

Auditor: Personas que intervendrán en la auditoría.

Características: Cualidades que tiene la empresa a evaluar.

Conclusiones: Determinación del grado de confiabilidad de los procedimientos de control que se llevan a cabo.

Conclusiones de recomendaciones: Determinación del enfoque a seguir en la auditoría.

Controles: Relación existente entre objetivos y procedimientos de control.

Costos: Costo que ocasionaría un paro o falla del sistema computarizado.

Cuestionario: Documento que permite conocer y analizar a base

de preguntas los procedimientos de controles.

Departamentos: Areas que utilizan los sistemas computacionales.

Especificaciones: Características del computador (proveedor, modelo, capacidad, ubicación).

Evaluación: Medida de cumplimiento o incumpliento de los procedimientos de control.

Giro de la empresa: Objeto por la cual está en operación la empresa.

Horas: Presupuesto de horas para llevar a cabo la auditoría.

Impacto de sistemas: Impacto que tiene el sistema en la organización.

Lenguaje: Lenguaje en que se desarrollan los sistemas.

Madurez: Nivel y tecnología que tienen los sistemas computarizados.

Objetivos de control: Metas de control que deben establecerse en la organización.

Personal: Número de personas que laboran en el área de sistemas.

Plan de auditoría: Reunión de planificación en la cual participa el socio , gerente y senior de auditoría. Sirve para determinar el enfoque a seguir en la auditoría.

Preguntas : Serie de cuestionamiento referentes a la existencia de procedimientos de control.

Procedimientos de control: Conjunto de técnicas aplicados para alcanzar los objetivos.

Procesos: Número de procesos computarizados.

Prueba: Conjunto de técnicas y procedimientos aplicables para medir el grado de confiabilidad del sistema.

Recomendaciones: Sugerencias posibles de establecer para la auditoría.

Relevancia: Relevancia del sistema computarizado.

Reporte de evaluación: Documento que permite conocer y analizar la situación de controles generales.

Reporte de pruebas: Respuestas a la aplicación de pruebas de auditoría.

Reporte de resultados: Documento que permite analizar el impacto del PROCESAMIENTO ELECTRONICO DE DATOS en la organización.

Respuestas: Serie de contestaciones al cuestionario.

Resultados: Respuestas que proporcionan información con respecto al cumplimiento en los procedimientos de control.

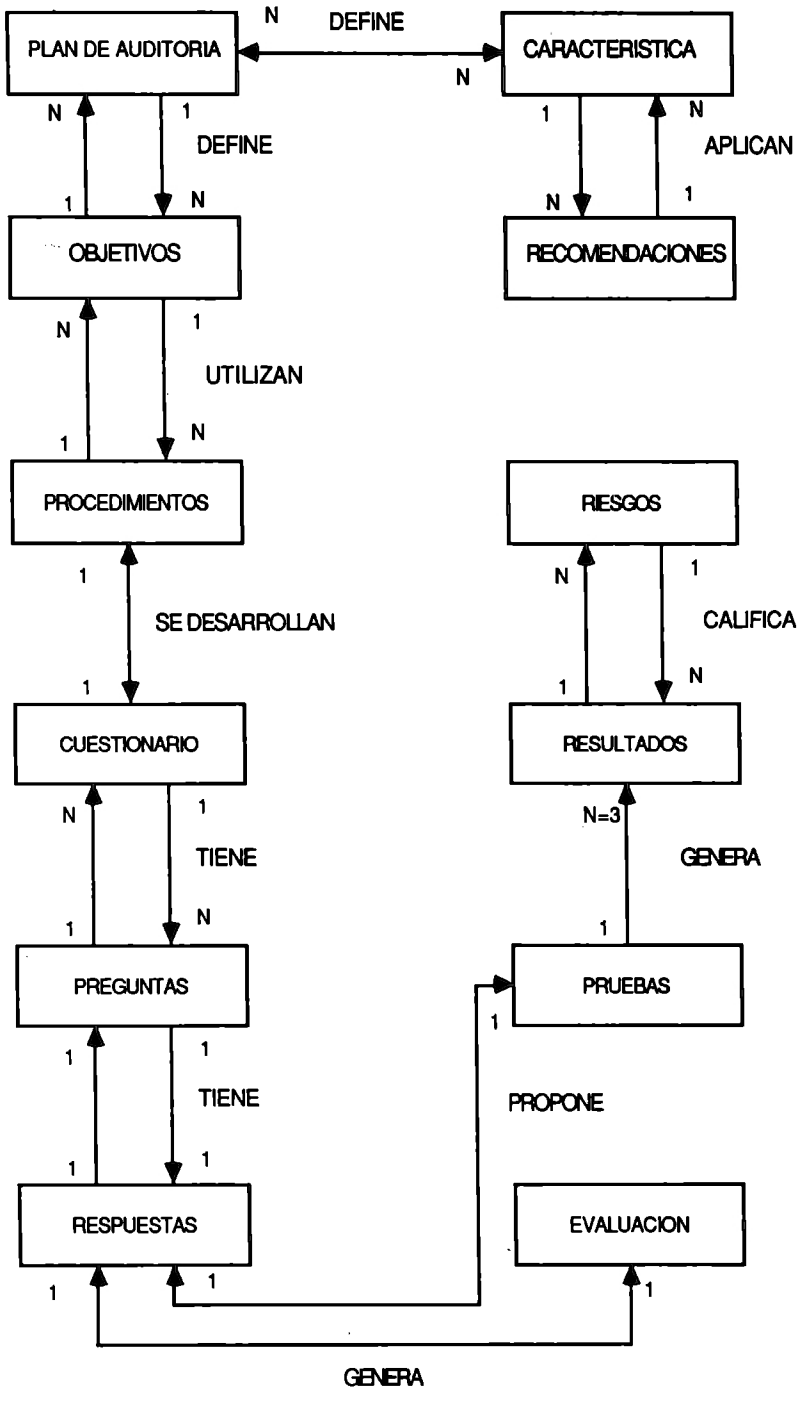
Resultado de prueba: Respuesta a la aplicación de pruebas de auditoría.

Riesgos: Impacto de la falta de procedimientos de control.

Terminales: Número de terminales utilizadas por el sistema.

Tipo de auditoría : Característica de la auditoría a realizar (financiera, operacional, administrativa).

DIAGRAMA ENTIDAD-RELACION



5.- PAQUETE DE DISEÑO

5.1 Lista de Miniespecificaciones

1.- Determinación de las características de Auditoría.

1.1.1 Detalle de información.

1.2.1 Explosiona programa.

1.2.2 Análisis de recomendaciones.

1.2.3 Elaboración de plan de enfoque.

2.- Determinación de las características de Controles Generales.

2.1.1.1 Obtención de objetivos de control.

2.1.1.2 Obtención de procedimientos de control.

2.1.2.1 Explosiona programa.

2.1.2.2 Generación del cuestionario.

2.2.1.1 Detalle de información

2.2.1.2 Explosiona programa.

2.2.1.3 Generación del reporte de evaluación.

2.2.1.4 Análisis de evaluación.

3.- Determinación de las pruebas de Auditoría.

3.1 Explosiona programa.

3.2 Generación de pruebas.

4.- Evaluación de resultados.

4.1.1 Detalle de la información.

4.1.2 Explosiona programa.

4.1.3 Generación de resultados.

4.2 Evaluación global de Controles Generales.

1.1.1 DETALLE DE INFORMACION

Entradas: Cédula de características de la empresa a evaluar.

Salidas: Información específica de las características de la empresa.

Proceso:

-Selecciona, de la cédula de características, información específica.

-Captura de información específica.

-Almacena en el archivo de características.

1.2.1 EXPLOSIONA PROGRAMA

Entrada: Información específica de las características de la empresa.

Salida: Recomendaciones.

Proceso:

-Ingresa características.

-Lee el archivo de recomendaciones.

-Selecciona recomendaciones.

-Almacena características y recomendaciones en archivo de Ref_Permanente.

1.2.2 ANALISIS DE RECOMENDACIONES

Entrada: Recomendaciones.

Salida: Conclusiones de recomendaciones.

Proceso:

-Lee recomendaciones.

-Analizar Recomendaciones.

-Determinación del enfoque a seguir en la Auditoría.

1.2.3 ELABORACION DEL PLAN DE ENFOQUE

Entradas: Conclusiones de recomendaciones.

Salida: Plan de Auditoría.

Proceso:

-Lee conclusión de recomendaciones.

-Analiza conclusiones

-Elaboración del Plan de Auditoría.

2.1.1.1 OBTENCION DE OBJETIVOS DE CONTROL

Entradas: Plan de Auditoría.

Salidas: Objetivos de control.

Proceso:

-Entrada del Plan de Auditoría.

-Despliega el menú de áreas de objetivos de control.

-En base al Plan de Auditoría selecciona áreas de objetivos de control.

-Lee el archivo de objetivos.

-Selecciona objetivos de control.

-Define objetivos de Control.

2.1.1.2 OBTENCION DE PROCEDIMIENTOS DE CONTROL

Entrada: Objetivos de control.

Salida: Controles.

Proceso:

-Ingresa objetivos de control.

-Lee archivo de procedimientos.

-Selecciona procedimientos de control.

-Define controles.

2.1.2.1 EXPLOSIONA PROGRAMA

Entradas: Controles.

Salidas: Preguntas.

Proceso:

-Ingresa controles.

-Lee archivo de cuestionario.

-Selecciona pregunta(s) del archivo de cuestionario para cada control (relación objetivo-procedimiento).

-Determina las preguntas para el cuestionario.

2.1.2.2 GENERACION DEL CUESTIONARIO

Entradas: Preguntas.

Salida: Cuestionario.

Proceso:

-Ingresa preguntas.

-Imprime cuestionario.

2.2.1.1 DETALLE DE INFORMACION

Entrada: Respuestas.

Salidas: Respuestas.

Proceso:

-Selecciona respuestas.

-Captura de respuestas.

-Almacena respuestas.

2.2.1.2 EXPLOSIONA PROGRAMA

Entradas: Respuestas.

Salidas: Resultados.

Proceso:

-Lee archivo de respuestas.

-Genera evaluación

-si respuesta = B entonces

el procedimiento de control es bueno.

-si respuesta = R entonces

el procedimiento de control es regular.

-si respuesta = M entonces

el procedimiento de control es malo.

-si respuesta = NE entonces

el procedimiento de control no existe.

-Almacena evaluación en archivo Ref_Permanente.

2.2.1.3 GENERACION DEL REPORTE DE EVALUACION

Entradas: Resultados.

salidas: Reporte de evaluación.

proceso:

-Ingresa evaluación.

-Imprime evaluación.

2.2.1.4 ANALISIS DE EVALUACION

Entrada: Reporte de evaluación.

Salida: concluciones.

Proceso:

-Lee reporte de evaluación.

-Determina grado de confiabilidad de controles.

-Genera conclusiones.

3.1 EXPLOSIONA PROGRAMA

Entradas: Respuestas.

Salidas: Pruebas.

Proceso:

-Lee archivo de respuestas.

-Genera pruebas

-si respuesta = B entonces

selecciona prueba para verificar.

-si respuesta = R entonces

selecciona prueba para verificar.

-si respuesta = M ó NE entonces

selecciona prueba para buscar control complementario.

-Almacena pruebas en archivo Ref_Permanente.

3.2 GENERACION DE PRUEBAS.

Entradas: Pruebas.

Salida: Reporte de pruebas.

Proceso:

-Ingresa pruebas.

-Imprime reporte de pruebas.

4.1.1 DETALLE DE LA INFORMACION

Entradas: Resultados de pruebas.

Salidas: Resultados de pruebas.

Proceso:

-Selecciona resultados de pruebas.

-Captura de resultados de pruebas.

-Almacena Resultados de pruebas en el archivo de resultados.

4.1.2 EXPLOSIONA PROGRAMA

Entradas: Resultado de pruebas.

Salidas: Riesgos.

Proceso:

-Lee archivo de resultados.

-Lee archivo de riesgos.

-Determinación de riesgos.

-si resultado = satisfactorio entonces

no hay riesgos.

-si resultado = regular entonces

determina riesgos posibles.

-si resultado = Malo entonces

determina la existencia de riesgos.

-Almacena riesgos en archivo Ref_Permanente.

4.1.3 GENERACION DEL REPORTE DE RIESGOS

Entradas: Riesgos.

Salidas: Reporte de riesgos.

Proceso:

-Ingresa riesgos.

-Imprime reporte de riesgos.

4.2 EVALUACION GLOBAL DE CONTROLES GENERALES

Entrada: Riesgos y conclusiones.

Salida: Reporte de evaluación.

Proceso:

-Lee riesgos y conclusiones.

-Analiza riesgos y conclusiones.

-Evalua riesgos y conclusiones.

-Genera evaluación.

5.2 Diseño de la Base de Datos

La base de datos sera diseñada siguiendo las características del modelo relacional.

5.2.1 Entidades y atributos

ENTIDAD: CARACTERISTICAS

Es un archivo que almacenará todas las características de la empresa a evaluar.

ATRIBUTOS:

Descripción:
No. de característica : llave
Nombre de la empresa.
Giro de la empresa
Tipo de Auditoría
Areas
Impacto de sistemas
Madurez
Departamentos
Especificaciones
Lenguaje
Relevancia

Terminales

Actividades

ENTIDAD: CUESTIONARIO

Es un archivo que esta integrado por las preguntas para verificar si se desarrollan los procedimientos de control.

ATRIBUTOS

Descripción:

Número de pregunta : llave

Pregunta

ENTIDAD: EVALUACION

Es un archivo que esta integrado por la evaluación de las respuestas del cuestionario.

ATRIBUTOS

Descripción:

No. de evaluación

Evaluación

ENTIDAD: OBJETIVOS

Es un archivo que esta integrado por todos los objetivos de control en forma general que debe tener implementado la empresa a evaluar

ATRIBUTOS

Descripción:
Area de control : llave
Número de objetivo : llave secundaria
Objetivo de control

ENTIDAD: PROCEDIMIENTOS

Es un archivo que esta integrado por todos los procedimientos de control generales que debe tener implementado la empresa a evaluar

ATRIBUTOS

Descripción:
No. de objetivo : llave
Número de procedimiento : llave secundaria
Procedimiento de control

ENTIDAD: PRUEBAS

Es un archivo que esta integrado por las pruebas de auditoría para verificar la confiabilidad del sistema.

ATRIBUTOS

Descripción:
Número de prueba
Prueba

ENTIDAD: RECOMENDACIONES

Es un archivo que está integrado por las sugerencias posibles a establecer para la auditoría.

ATRIBUTOS

Descripción:
No. de característica : llave
Recomendaciones : llave secundaria
Auditor
Horas

ENTIDAD: REF_PERMANENTE

Es un archivo que almacenará las recomendaciones, las pruebas, evaluación y los riesgos del sistema que se este evaluando.

ATRIBUTOS:

Descripción:
Nombre de la empresa : llave
Recomendaciones
Pruebas
Evaluación
Riesgos

ENTIDAD: RESPUESTAS

Es un archivo que almacenará las respuestas obtenidas a través del cuestionario.

ATRIBUTOS:
Descripción:
No. de respuesta : llave
Respuesta : llave secundaria
Número de pregunta

ENTIDAD: RESULTADOS
Es un archivo que almacenará los resultados obtenidos a través de las pruebas efectuadas.

ATRIBUTOS:

Descripción:

Resultado : llave

Número de prueba

ENTIDAD: RIESGOS

Es un archivo que esta integrado por los riesgos posibles por falta de controles generales.

ATRIBUTOS

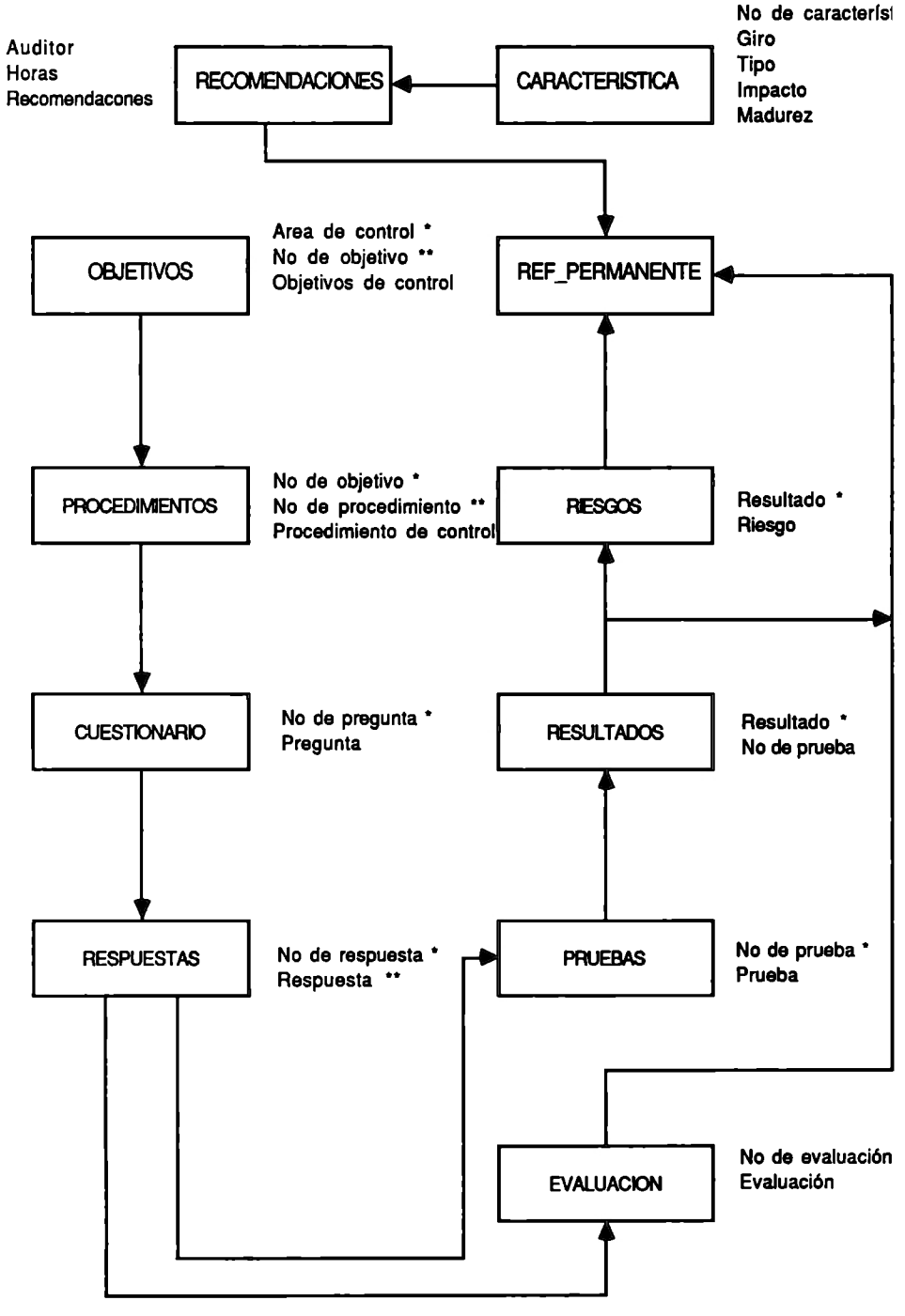
Descripción:

Resultado : llave

Número de prueba

Riesgos

DIAGRAMA DE LA BASE DE DATOS



CONCLUSIONES

Día con día aumentan los sistemas computarizados de información y el auditor tradicional necesita conocer más de estos . La capacitación debe formar parte del desarrollo profesional del auditor, sin embargo no todos tienen la capacidad de cambiar rápidamente. Considero que este sistema no sólo puede ser utilizado por el auditor especialista en informática sino también por aquellos auditores que les cuesta trabajo el cambio.

Siempre y cuando sea bien contestado la guía de evaluación de control interno los resultados de la evaluación serán los esperados.

Hay en la actualidad despachos de contadores públicos que utilizan sistemas de soporte de decisiones para el estudio y evaluación del control interno del área de procesamiento electrónico de datos.

A continuación presento las conclusiones que a mi juicio considero forman parte de los resultados del presente documento:

1.- La automatización de los sistemas de información no

representan un cambio en los objetivos de la auditoría, lo que cambian son las herramientas y técnicas utilizadas por el auditor para alcanzar estos objetivos.

2.- Las normas de auditoría generalmente aceptadas son fundamentales en su aplicación, aunque existan normas de auditoría de sistemas de información debido al nivel de contenido que en éstas se expresa.

3.- El profesional de auditoría debe de tener conocimentos básicos para que tenga herramientas suficientes para poder efectuar su trabajo con capacidad y con el soporte que le da el entrenamiento técnico. Esto no significa que tenga que ser un experto en sistemas de información.

4.- Las necesidades de revisar y evaluar controles generales en el área de procesamiento electrónico de datos es clara e importante. El no hacerlo, o efectuarlo en forma pobre, implica que los riesgos de una opinión o informe mal fundado se incremente.

5.- Las instituciones encargadas de la educación técnica de especialistas en auditoría, es decir, Contadores Públicos, no se han preocupado por el cambio actual en los sistemas administrativos y financieros. A raíz de lo anterior se

carece de una adecuada preparación en auditoría de sistemas de información automatizados. Seria prudente que los planes de estudios se actualizaran de tal forma que contengan materias destinadas a la capacitación en auditoría de sistemas. Ya que la auditoría tradicional esta siguiendo tendencias hacia la especialización en sistemas de información.

6.- El auditor no sólo debe de revisar y evaluar los sistemas de información automatizados sino también convertirlos en herramientas útiles que le proporcionen conocimientos y experiencias que lo soporten en la toma de decisiones. Esto va a abrir la posibilidad de que los Sistemas de Soporte de Decisiones se conviertan en dichas herramientas.

7.- El sistema de revisión de controles generales complementará o auxiliará en la capacitación de auditores en sistemas de información.

8.- El trabajo, considero que cumple el objetivo por el cual se planteo, ya que la herramienta como tal es muy útil, al mismo tiempo capacita al auditor y puede en un momento dado transmitir experiencias.

9.- Si el cuestionario de control interno para la revisión de controles generales no es contestado en forma correcta, el sistema no será de gran ayuda para el auditor como efecto de lo mismo. Recordemos que el que alimentará en un momento dado al sistema es el auditor y si lleva vicios en su alimentación o ejecución del trabajo de recopilación de respuestas a través del cuestionario los resultados emitidos por el sistema no serán los deseados.

BIBLIOGRAFIA

A Practical guide to EDP auditing
AUERBACH Publishers Inc.
USA. 1982.

Burch John A.
"Computer control and auditing"
John Wiley and Sons, Inc.
USA. 1978.

CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS
"Procedimientos de Control en Computación"
Instituto Mexicano de Contadores Públicos A.C.
México, 1979.

INSTITUTO MEXICANO DE CONTADORES PUBLICOS, A.C.
"Efectos del Procesamiento Electrónico de Datos (PED) en el Examen del Control Interno"
México, 1984.

INSTITUTO MEXICANO DE CONTADORES PUBLICOS, A.C.
"Normas y Procedimientos de Auditoría"
México, 1984.

Krauss Leonard I.
"Security Audit and Field Evaluation for Computer Facilites and Information (SAFE)"
AMACOM
USA, 1980.

Lott Richard
"Auditoría y Control del Procesamiento de Datos"
NORMA
Colombia, 1984.

Mancera Hermanos y Cía. S.C.
"Guía para la evaluación de los controles generales"
Arthur Young International.

Perry William E.
"A Standard for Auditing Computer Applications.- Selected Audit Areas"
AUBERBACH PUBLISHERS INC.
USA, 1986.

Solís Gustavo y Pozos José
Tesis de Licenciatura: "Introducción a la Auditoría en Informática"

Universidad Nacional Autónoma de México
Facultad de Estudios Superiores "Cuautitlán"
México, 1983.

Weber Ron
EDP Auditing. Conceptual Foundations and Practice
McGraw Hill Inc.
Singapore, 1985.

Yourdon Edward
Managing The System Life Cycle
Prentice Hall, Yourdon Press. 2a. Edición
USA. 1988.

APENDICE I

GUIA DE EVALUACION PARA LA REVISION DE CONTROLES GENERALES

I ORGANIZACION

Independencia del área de informática

1.- El área cuenta con un organigrama completo, formal y actualizado ?

B- Existe formalmente
R- Existe pero no se encuentra autorizado
M- Existe formalmente pero no está actualizado
NE- No existe

2.- El nivel jerarquico del área de informática es adecuado con relación con sus usuarios ?

B- Nivel mayor o igual a sus usuarios
R- No procede
M- No procede
NE- Depende de un usuario

Segregación de funciones

3.- Existe una adecuada segregación de funciones entre PED y sus usuarios ?

B- Es formal y se respeta
R- No es formal pero se respeta
M- La segregación no es consistente
NE- No existe segregación de funciones

4.- Los operadores realizan actividades de programación?

B- Nunca programan
R- Programan eventualmente
M- Programan normalmente
NE- La programación forma parte de sus funciones

5.- Los programadores realizan actividades de operación de sistemas ?

B- Nunca operan los sistemas
R- Operan eventualmente
M- Operan normalmente
NE- Operan como parte de sus funciones

6.- Se cuenta con una completa y actualizada descripción de funciones para el área de sistemas ?

B- Si se cuenta
R- No estan actualizadas o autorizadas
M- El personal no las conoce
NE- No existen

7.- El personal de PED realiza operaciones de compra-venta de equipo y accesorios ?

B- Nunca las realiza
R- Las hace eventualmente
M- Las hace formalmente
NE- Forma parte de sus funciones

8.- El personal de PED tiene capacidad para autorizar el inicio de transacciones financieras ?

B- Nunca lo hace
R- Lo hace eventualmente
M- Lo hace regularmente
NE- Forma parte de sus funciones

Adecuada inversiones en procesamiento de datos

9.- Se efectuan estudios de viabilidad que soporten la adquisición de equipos y sistemas ?

B- Existen estudios completos y autorizados
R- Existen estudios completos sin autorizar
M- Existen pero incompletos
NE- No existen

10.- Los equipos instalados corresponden a los resultados de dicho estudio ?

B- Si corresponden
R- Son equivalentes
M- No procede
NE- No corresponden

II ADMINISTRACION

Dirección de las funciones de Procesamiento Electrónico de Datos

11.- Se cuenta con un manual de políticas y procedimientos del área ?

B- Existe formalmente actualizado y es conocido por el personal
R- Existe informal, pero esta actualizado y es conocido por el personal
M- Existe desactualizado
NE- No existe

Planeación de las funciones de Procesamiento Electrónico de Datos

12.- Existe un plan de sistemas a corto y largo plazo ?

B- Existe plan formal a corto plazo y largo plazo
R- Existe plan formal a corto plazo
M- Existen planes informales
NE- No existe planeación de sistemas

13.- Existen procedimientos para el desarrollo de las actividades del plan ?

B- Son formales y se llevan a cabo
R- Son informales pero se respetan
M- No son utilizados
NE- No existen

Adecuada comunicación entre Procesamiento Electrónico de Datos y usuarios

14.- Se realizan reuniones periodicas enre PED y sus usuarios ?

B- Se realizan formalmente
R- Se realizan informalmente
M- Se realizan irregularmente
NE- No se realizan

Control Financiero del Area de Procesamiento Electrónico de Datos

15.- Se cuenta con un presupuesto autorizado del área ?

B- Existe autorizado
R- Existe sin autorizar
M- No precede
NE- No existe

16.- Se ejerce control sobre el ejercicio del presupuesto ?

B- Se ejerce control adecuado
R- No procede
M- Se ejerce control inadecuado
NE- No se ejerce control

Supervisión del área de sistemas

17.- Existen revisiones de auditoría interna a PED ?

B- Revisiones de control interno y desarrollo de pruebas
R- Revisiones de controles generales y específicos
M- Revisión de controles generales
NE- Ninguna participación

III DESARROLLO DE SISTEMAS

Estandarización de las funciones de informática

18.- Se cuentan con estándares para el análisis y diseño de sistemas ?

B- Existen estándares y se respetan
R- No son formales pero se respetan
M- Los estándares no se respetan
NE- No existen estándares

19.- Existen estándares para la prueba de sistemas ?

B- Existen estándares y se respetan
R- No son formales pero se respetan
M- Los estándares no se respetan
NE- No existen estándares

20.- Existen estándares para la implantación de sistemas ?

B- Existen estándares y se respetan
R- No son formales pero se respetan
M- Los estándares no se respetan
NE- No existen estándares

21.- Existen estándares para modificaciones a sistemas en producción ?

B- Existen estándares y se respetan
R- No son formales pero se respetan
M- Los estándares no se respetan
NE- No existen estándares

22.- Se cuenta con estándares de documentación ?

B- Existen estándares y se respetan
R- No son formales pero se respetan
M- Los estándares no se respetan
NE- No existen estándares

23.- Existen estándares para programación ?

B- Existen estándares y se respetan
R- No son formales pero se respetan
M- Los estándares no se respetan
NE- No existen estándares

24.- Se tienen estándares para la nomenclatura de programas, archivos, bibliotecas y listados ?

B- Existen estándares y se respetan
R- No son formales pero se respetan
M- Los estándares no se respetan
NE- No existen estándares

Cambios a los sistemas

25.- Existe una requisición formal del usuario ?

B- Existen requisiciones formales
R- No procede
M- No siempre son formales
NE- No hay requisiciones formales

26.- Las pruebas se efectuan sobre copias de programa fuente?

B- Siempre se utilizan copias
R- Eventalmente se utilizan los originales
M- No procede
NE- Se utiliza indistintamente copias u originales

27.- Las pruebas no se realizan sobre archivos reales ?

B- Nunca se utilizan archivos reales
R- Eventualmente se utilizan
M- No procede
NE- Se uilizan indistintamente

28.- Las pruebas son verificadas y autorizadas ?

B- Siempre se verifican y autorizan
R- Se verifican pero no se autorizan
M- No se verifican
NE- No se realizan pruebas

Control sobre análisis y desarrollo de sistemas

29.- El usuario participa en la definición de objetivos y características generales de los sistemas ?

B- Participa activa y continuamente
R- Participa limitadamente
M- Participa en forma pasiva
NE- Nunca participa

30.- Se efectuan pruebas a los sistemas antes de liberarlos ?

B- Siempre se realizan pruebas formales
R- Se realizan pruebas informales
M- No procede
NE- No siempre se realizan pruebas

31.- Los sistemas son documentados ?

B- Se documentan oportunamente
R- Se documentan después de su liberación
M- No procede
NE- No se documentan

Controles sobre la implantación de sistemas

32.- Existen procedimientos y estándares para la conversión e implantación ?

B- Existen y se respetan
R- No existen pero se efectuan adecuadamente
M- No se respetan los estándares
NE- No existen

Documentación suficiente para la operación de sistemas

33.- La documentación de cada sistema cuenta con manual del sistema de operación y del usuario ?

B- La documentación se encuentra completa, actualizada y bajo estándares
R- La documentación esta incompleta o desactualizada
M- La documentación esta incompleta y desactualizada
NE- No existe documentación

V OPERACION DE SISTEMAS

Controles sobre los trabajos procesados

34.- Existe un calendario de producción ?

B- Existe y se respeta
R- No existe formalmente
M- Existe pero no se respeta
NE- No existe calendario

35.- Se cuenta con procedimientos para la asignación de prioridades ?

B- Existen y se respetan los procedimientos
R- Existen procedimientos adecuados pero son informales
M- No se respetan los procedimientos
NE- No hay procedimientos

36.- Existe una función de bibliotecario independiente a operación?

B- Si es independiente
R- No procede
M- No procede
NE- No es independiente

37.- Procesamiento Electrónico de Datos no efectua correciones a los documentos fuente ?

B- No se efectuan correciones
R- No procede
M- No procede
NE- Si se llegan a efectuar

38.- Los discos, cintas y diskettes cuentan con etiquetas externas de identificación ?

B- Si se tienen
R- Algunos dispositivos las tienen
M- No procede
NE- No se cuenta con etiquetas externas

Continuidad en la operación de los sistemas

39.- Existe un registro de fallas y control del servicio de mantenimiento correctivo al equipo ?

B- Existe formalmente
R- Existe pero en forma informal
M- No procede
NE- No existe

V SEGURIDAD

Salvaguarda de los activos

40.- Las instalaciones de PED están en lugares públicos ?

B- No están a la vista del público
R- No procede
M- No procede
NE- Si están a la vista del público

41.- El acceso al área de PED se limíta a personal del propio departamento ?

B- Procedimientos formales y se respetan
R- Procedimientos informales pero se respetan
M- Procedimiento formal pero no se respeta
NE- No existe restricción

42.- Se cuenta con equipo de detección de humo ?

B- Existe
R- No procede
M- Existe pero no funciona
NE- No existe

43.- No existe material inflamable en el centro de cómputo ?

B- No existe
R- No procede
M- No procede
NE- Si existe

Continuidad del procesamiento ante contingencias

44.- Existe un plan de contingencias para informática ?

B- Existe completo y se conoce
R- Existe pero no se conoce
M- Se encuentra en desarrollo
NE- No existe plan

45.- Se cuenta con una póliza de seguro adecuada ?

B- Existe y es adecuada
R- Existe pero es incompleto
M- No procede
NE- No existe

46.- Existe equipo que evite la pérdida de información a pesar de fallas en el suministro de energía eléctrica (NO BREAK) ?

B- Existe
R- No existe equipo pero si procedimientos
M- No procede
NE- No existe equipo

47.- Existen respaldos de archivos programas, sistemas operativos y documentación ?

B- Existen respaldos completos
R- No existe de todo el material o no está actualizado.
M- No procede
NE- No existen respaldos

48.- El material de respaldo está accesible a cualquier hora ?

B- Accesible a toda hora
R- No procede
M- No procede
NE- No es accesible a toda hora

Asegurar la integración de la información

49.- Existen áreas exclusivas para el desarrollo y prueba de los programas ?

B- Existe disposición y se cumple
R- No existe disposición pero existe separación
M- Existe disposición pero no se cumple
NE- No existen áreas exclusivas

50.- Existe un sistema de passwords de acceso ?

B- Si existe
R- No procede
M- No procede
NE- No existe

51.- El sistema detecta y registra intentos no autorizados de acceso al equipo ?

B- Si detecta y registra
R- Si detecta pero no registra
M- No procede
NE- No detecta ni registra

52.- Se ejerce un adecuado control sobre la entrada y salida de cintas, discos y diskettes ?

B- Si hay adecuado control
R- No procede
M- No procede
NE- No hay control

APENDICE II

PROCEDIMIENTOS DE AUDITORIA PARA LA REVISION DE CONTROLES GENERALES

I y II Organización y Administración

1.- Discución con la dirección y la gerencia

2.- Papeles de trabajo de auditoría interna

3.- Inspección de:

- Organigramas
- Manuales
- Planes (estratégico, de capacitación)
- Descripción de puestos
- Minutas de comités
- Estudios de viabilidad
- Pólizas de seguro

4.- Revisión de presupuestos

III Desarrollo y Mantenimiento de Sistemas

1.- Inspeccionar estándares escritos sobre funciones del Area

2.- Evaluar los estándares (si cumplen con los objetivos de control)

- Participación del usuario
- Evaluación lógica-económica

- Aprobación de proyecto
- Seguimiento del desarrollo
- Autorización de pruebas
- Aprobación del usuario
- Catalogación de modificaciones
- Documentación de cambios
- Implantación y seguimiento
- Postevaluación

3.- Inspeccionar documentación de los sistemas, a nivel:

- Sistema
- Programas
- Operación
- Usuario

4.- Verificar cumplimiento de la documentación física vs. estándares

5.- Verificar (sobre muestras) lo correcto y autorizado de:

- Solicitudes de cambios
- Aprobación de cambios
- Autorización de catalogación en producción
- Documentacion de cambios

6.- Verificar la correcta segregación de funciones del área

IV Operación

1.- Verificar la existencia de manuales de operacion

2.- Verificar la existencia de un calendario de producción

3.- Verificar la existencia de una botácora del sistema

4.- Comparar selectivamente bitácora de operación vs. calendario de producción

5.- Obtener un listado de catalogaciones recientes de programas y comprobar su soporte documental

6.- Verificar la existencia de un reporte de mantenimiento preventivo y correctivo

7.- Visitar las instalaciones de servicio y verificar su correcto funcionamiento

8.- Inspeccionar el almacén de cintas y discos magnéticos

9.- Verificar la existencia de etiquetas externas

10.- Selectivamente, verificar las etiquetas externas vs. el VTOC (directorio) de los dispositivos

11.- Verificar el control sobre las cintas scrath

12.- Inspeccionar las instalaciones y material de respaldo

13.- Verificar la correcta distribución de costos/gastos

V Sistema operativo y Base de datos

1.- Identificar a los responsables del software de la instalación, y obtener información sobre políticas y procedimientos del área

2.- Inspeccionar documentación del software

3.- Verificar la corrección de la organización de la base de datos

4.- Verificar la definición de funciones y responsabilidades del administrador de la base de datos

5.- Verificar la observancia de estándares

VI Seguridad física y lógica

1.- Visitar e inspeccionar lo adecuado de las instalaciones

2.- Verificar el control del acceso al área y centro de cómputo

3.- Visitar las instalaciones de respaldo y verificar lo adecuado y disponible de las mismas

4.- Obtener conocimiento sobre el sistema de passwords. Verificar lo adecuado del mismo

5.- Obtener la lista de usuarios activos del sistema y verificar su justificación

6.- Obtener una relación de usuarios y niveles de acceso y verificar lo adecuado de los mismos de acuerdo a sus funciones

7.- Verificar la existencia de áreas independientes de desarrollo, prueba y producción

8.- Verificar la distribución básica de programas fuente y objeto en producción

9.- Obtener listado de programas fuente y programas objeto de un sistema y verificar la correspondencia entre los mismos y con la documentación del sistema

10.- Con base en un programa fuente:

- Compilar y obtener reporte
- Verificar la ausencia de errores
- Comparar reporte contra documentación del sistema
- Por medio de software, comparar el programa fuente en producción. Y el programa objeto generado vs. el programa objeto en producción

11.- Obtener un listado de archivos y bibliotecas y verificar su nivel de protección y su corrección de acuerdo a la documentación del sistema