



UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

"FUNDAMENTOS DE AUDITORIA
EN INFORMATICA"

T E S I S

QUE PARA OBTENER EL TITULO DE:
LICENCIADA EN CONTADURIA
P R E S E N T A:
ALICIA CARRANZA TELLEZ
ASESOR: L.A. PEDRO BRAVO ARAIZA

**TESIS CON
FALLA DE ORIGEN**

CUAUTITLAN IZCALI, EDO. DE MEX.

1996

**TESIS CON
FALLA DE ORIGEN**



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



ESTADOS UNIDOS MEXICANOS
 FEDERAL NACIONAL
 DE ESTUDIOS SUPERIORES
 DE CUAUTITLAN

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
 UNIDAD DE LA ADMINISTRACION ESCOLAR
 DEPARTAMENTO DE EXAMENES PROFESIONALES

FACULTAD DE ESTUDIOS
 SUPERIORES-CUAUTITLAN

ASUNTO: VOTOS APROBATORIOS



DEPARTAMENTO DE
 EXAMENES PROFESIONALES

DR. JAIME KELLER TORRES
 DIRECTOR DE LA FES-CUAUTITLAN
 P R E S E N T E .

AT'N: Ing. Rafael Rodríguez Ceballos
 Jefe del Departamento de Exámenes
 Profesionales de la F.E.S. - C.

Con base en el art. 28 del Reglamento General de Exámenes, nos permitimos comunicar a usted que revisamos el trabajo "Fundamentos de Auditoría en Informática".

que presenta la pasante: Carranza Téllez Alicia,
 con número de cuenta: 8709348-8 para obtener el TITULO de:
Licenciada en Contaduría.

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VOTO APROBATORIO.

A T E N T A M E N T E .
 "POR MI RAZA HABLARA EL ESPIRITU"
 Cuautitlan Izcalli, Edo. de Méx.; a 29 de Enero de 1976.

PRESIDENTE	<u>L.A. Pedro Bravo Araiza</u>	
VOCAL	<u>C.P. J. Luis Covarrubias Guerrero</u>	
SECRETARIO	<u>L.A. Pedro Everardo Vargas Reyes</u>	
1er. SUPLENTE	<u>L.A. Araceli Nivon Zaghi</u>	
2do. SUPLENTE	<u>L.A. Teresa Amador Pérez</u>	

Considero que los logros del ser humano son producto de la enseñanza que haya adquirido durante toda su vida, a través de los grupos con quienes se mantiene relacionado, son quienes transmiten su filosofía de la vida y generación, moldeando así, un carácter y alentando el espíritu.

Llegar hasta esta etapa de mi vida en una satisfacción y sobre todo un logro que hoy comparto con la gente que de alguna manera me ha instruido en lo material, moral y espiritual.

Por lo que respecta al desarrollo académico agradezco a mi alma mater la U.N.A.M. por la oportunidad que me brindó al abrirme sus puertas, a todos mis profesores que formaron en mí un estricto sentido de servicio profesional en particular deseo expresar mi más profundo agradecimiento por las aportaciones que hiciera en la elaboración del presente trabajo de tesis al Lic. Pedro Bravo Araiza y al Ing. Ernesto Franco.

A mi sínodo examinador, por la paciencia e interés que mostraron en la revisión de esta investigación y los valiosos comentarios que de ellos he recibido, mi gratitud.

Deseo hacer especial mención y reconocimiento a un grupo importante, un equipo que ha sido columna vertebral de mi vida y a quienes hoy deseo expresar mi más profundo amor, admiración y respeto. Mi familia.

Primariamente están aquellos a quienes busco y siempre encuentro, a quienes ni las limitaciones, ni los sacrificios ni nada han impedido apoyar el progreso de cada uno de sus miembros. A esa parte la familia que me recibió con el mismo amor que Dios les dio, quienes me enseñaron a caminar, hablar, sentir, etc.. Siempre con esa misma enseñanza y ejemplo, mi más profundo reconocimiento a mi MADRE y PADRE.

A dos personas tan especiales que son mi futura familia a quienes amo y agradezco infinitamente que compartan esta etapa de mi vida, la primera es mi futuro esposo que ha sido más que un amigo, compañero y novio ya que he tenido en todo momento su apoyo de cualquier tipo desinteresadamente, mil gracias por dejarme aprender de ti, Gerry. La siguiente personita, es mi bebé que me acompaña, dedico esto, con todo mi amor y cariño.

A mis hermanos, Luigi que ha sido como un segundo padre y a Beto les agradezco esos momentos tan importantes que hemos compartido. Gracias.

A Malenita y Ranin por sus cuidados, paciencia y gratitud. Gracias.

A mis primos lo único que les diría es que valoren y que aprovechen lo que tienen y lo que se les da.

A mis amigos, con quienes he compartido momentos alegres, de quienes he recibido apoyo en su momento dentro y fuera del quehacer académico, mi más profundo agradecimiento a esta segunda familia.

Índice de Contenido

Introducción

I. Concepto de Auditoría, Informática y Auditoría en Informática.	1
Concepto de Auditoría.	1
Concepto de Informática.	2
Concepto de Auditoría en Informática.	4
Diversos tipos de Auditoría y su relación con la Auditoría en Informática	8
II. Planeación de la Auditoría	11
Problemas que pueden surgir en la recopilación de información.	18
Definición y Objetivos del Control Interno.	21
Objetivos Básicos de control Interno.	21
Objetivos Generales del Control Interno.	22
Objetivos de Autorización.	23
Objetivos de Procedimiento y Clasificación de Transacciones.	23
Objetivo de Salvaguarda Física.	24
Objetivo de Verificación y Evaluación.	24
Programa de Trabajo.	28
Ventajas.	29
III. Auditoría de la Función de Informática.	31
Costo/Beneficio.	32
Controles Generales.	35
Evaluación de la Estructura Orgánica.	38
Organigrama Gerencial.	42
IV. Evaluación de los Sistemas	43
Mantenimiento.	51
Técnicas de Definición de Requerimientos.	53
Modelos Conceptuales.	56
Formalismo y Lenguajes de Especificación.	58
Diseño de la Arquitectura.	60
Identificación de Programas.	61
El Comportamiento Dinámico del Sistema.	61
Las Interacciones Organizacionales.	62
Las Responsabilidades.	62
Diagrama de Estructura.	62

Control de Calidad.	64
Norma de Especificación de requerimientos.	64
Criterio de Revisión y Aceptación de la Especificación de Requerimientos.	65
Herramientas de Elaboración y Almacenamiento de la Especificación de Requerimientos.	66
Sintáxis y Palabras Reservadas.	66
Normas de Codificación.	66
Herramientas Automáticas.	68
Auditor de Código.	69
Biblioteca de Soporte de programas.	70
Administración del Desarrollo de la Programación.	73
Complejidad de la Programación.	74
Métodos para el Control de la Calidad en el Desarrollo de Software.	74
Pruebas de Sistema.	78
Cuestionario.	84
V. Evaluación del Proceso de Datos y de los Equipos de Computo.	87
Tipos de Mantenimiento.	91
Cuestionario.	94
VI. Evaluación de la Seguridad	95
Riesgos.	101
Pérdidas y Fraude.	103
Fraude Informático.	105
Función de los Auditores Internos y Externos.	106
Auditores Internos.	107
Auditores Externos.	107
Funciones de Seguridad de la Auditoría en Informática.	109
Alcance de la Auditoría Respecto a la Seguridad en Informática.	110
Función de los Sistemas en Operación.	111
Instrucción y Capacitación.	112
Cuestionario.	115
Conclusiones.	
Glosario.	
Bibliografía.	

INTRODUCCION

En la actualidad los sistemas de información mediante la computadora constituyen una necesidad esencial, pero como saber si los equipos , el personal, el software y los sistemas con los que cuenta son, en realidad los adecuados.

Se cree que tiene que haber personal especializado dentro del área de informática, pero no necesariamente se requiere de esto, ya que solo intervendrá en el diseño general del sistema, diseño de controles, sistemas de seguridad, respaldo y confidencialidad del sistema y sistemas de verificación.

En algunas ocasiones se tiene poco control sobre la utilización de los equipos y un deficiente sistema de seguridad tanto física como lógica y falta de confidencialidad de la información.

Los ordenadores han pasado a formar parte integrante de los sistemas contables de muchas empresas. Estas máquinas realizan cálculos y funciones contables y son el único lugar en que se mantienen algunos de los registros financieros y operativos. Cada vez más se espera que el departamento financiero prepare los datos de entrada al sistema informático y utilice los de salida del mismo sistema. Los departamentos de informática y de proceso de datos realizan muchas de las funciones de control que van incorporadas en los sistemas. El grado de mecanización de la función contable variará de un lugar a otro, pero lo más probable es que sea considerable.

A todos los contables, incluidos los auditores, les preocupa la bondad del proceso, la exactitud de los datos grabados y la adecuación de los procedimientos de control. El ordenador participa en todos estos aspectos. Por consiguiente el auditor deberá adquirir los conocimientos necesarios para llevar a cabo los estudios de sistemas y aplicaciones mecanizados y verificar los datos que estén procesando.

La mayoría de los auditores estarán capacitados para verificar los datos de entrada al ordenador y utilizar los de salida, así como de hacer su trabajo de auditoría sobre sistemas mecanizados y solicitar la ayuda

de auditores informáticos con una preparación tecnológica más elevada.

Cualquiera que sea la especialización, deberá asegurarse que la auditoría sea completa. El sistema informático constituye tan sólo una parte del proceso total de auditoría e integrarse con sus trabajos.

OBJETIVOS

-Establecer los aspectos teóricos de la Auditoría en Informática en base a las Normas y Procedimientos con el fin de evaluar los sistemas de cómputo.

-Estudiar el sistema y analizar los controles organizativos y operativos del Departamento de Informática con el fin de optimizarlos.

-Analizar los sistemas de aplicación que se estén desarrollando o que ya estén implantados, con énfasis en el cumplimiento de las normas y procedimientos con que se diseñaron.

-Evaluar los programas, su diseño, el lenguaje utilizado, interconexión entre los programas y características del hardware empleado ya sea total o parcial para el desarrollo del sistema.

-Evaluar que el sistema de cómputo funcione conforme a las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación.

-Plantear un sistema de revisiones periódicas con un adecuado seguimiento de las observaciones para lograr las correcciones a los problemas y las mejoras a los sistemas que lo ameriten.

-Analizar los sistemas y procedimientos y de la eficiencia que se tiene en el uso de la información.

-Evaluar administrativamente el departamento para verificar si siguen correctamente las políticas implantadas.

-Dar a conocer a quienes dirigen o controlan el centro de cómputo medidas de seguridad para prevenir hechos delictuosos que destruyan el patrimonio empresarial.

HIPOTESIS

Si se analizan algunas funciones del departamento de informática se estará en posibilidad de estructurar el área funcional a que se hace referencia.

CAPITULO I

CONCEPTO DE AUDITORIA, INFORMATICA Y AUDITORIA EN INFORMATICA.

La palabra **auditoría** viene del latín auditorius, y de ésta proviene auditor, que tiene la virtud de oír, y el diccionario lo define como "revisor de cuentas colegiado". El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminando a un objetivo específico que es el de evaluar la eficiencia y la eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

El Boletín "C" de Normas y Procedimientos de Auditoría del Instituto Mexicano de Contadores Públicos nos dice:

"La auditoría no es una actividad meramente mecánica que implique la implicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo, son de carácter indudable. La auditoría requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben de seguirse y estimar los resultados obtenidos".

Así como existen normas y procedimientos específicos para la realización de auditorías contables, debe haber también normas y procedimientos para la realización de auditorías en informática como

parte de una profesión . Estas deben estar basadas con algunas características propias guiándose por el concepto de que la auditoría debe ser más amplia que la simple detección de errores, y además la auditoría debe evaluar para mejorar lo existente, corregir errores y proponer alternativas de solución.

El concepto de **informática** es más amplio que el simple uso de equipos de cómputo o bien de procesos electrónicos.

"No existe una sola concepción acerca de lo que es informática; etimológicamente, la palabra informática, deriva del francés informatique. Este neologismo proviene de la conjunción de information (información), y automatique (automática).¹

"Aplicación racional, sistemática de la información para el desarrollo económico, social y político".²

"Ciencia de la política de la información".³

"Ciencia de los sistemas inteligentes de información".⁴

1)Boletín del Centro de Informática de la F.C.A. de la U.N.A.M., número 99, Vol.11, Marzo 1984.

2 y 3) IBI (Oficina Intergubernamental de Informática, en aquel tiempo los 70's órgano asociado a la UNESCO).

4)Academia Mexicana de Informática (1977).

En algunas ocasiones se han empleado como sinónimos los conceptos de proceso electrónico, computadora e informática. La informática se considera, el total del sistema y el manejo de la información, la cual puede usar los equipos electrónicos como una de sus herramientas.

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

La información ha sido dividida en varios niveles:

1o Es el nivel técnico que considera los aspectos de eficiencia y capacidad de los canales de transmisión.

2o Es el nivel semántico y considera la información desde el punto de vista de su significado.

3o Es el pragmático y considera al receptor en un contexto dado.

4o Este considera la información desde el punto de vista normativo y considera cuándo, dónde y a quién se destina la información o la difusión que se le da.

La planeación y control de la información nos da nuevos aspectos muy importantes a considerar, entre los que están la teoría de sistemas, las bases de datos y los sistemas de información que van a contemplar el concepto de informática y su campo de acción.

Auditoría en Informática es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones; además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos seguridad y obtención de información.

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

Suele haber algunos auditores especializados en auditoría en informática, lo que limita la cantidad de personas de auditoría que han de recibir una formación profunda en auditoría en informática. La mayoría de los auditores estarán capacitados para verificar los datos de entrada al ordenador y utilizar los de salida, así como de hacer su trabajo de auditoría sobre sistemas mecanizados y solicitar la ayuda de auditores informáticos con una preparación tecnológica más elevada. Algunos auditores estarán preparados para evaluar sistemas de aplicaciones informáticas, revisar instalaciones y acceder a los archivos.

Unos pocos auditores que tengan mejor formación y mayor experiencia podrán tratar cuestiones técnicas, utilizar el ordenador y ayudar así a sus colegas.

El papel del auditor informático (que al fin y al cabo, es un miembro más del equipo de auditoría) va a ser variable. A todos los auditores informáticos les preocupará básicamente el control interno, el control y la seguridad de los activos de la empresa. Muchos auditores tendrán una gama de responsabilidad mucho más amplia, en la que se incluyan los análisis de los sistemas y de los estudios empresariales. Algunos se interesarán en la eficacia, eficiencia, continuidad de los sistemas y en la exactitud de los casos que se presenten en la jefatura. Además, otros auditores analizarán si el equipo informático y los sistemas de software son técnicamente adecuados y eficientes.

El trabajo de la auditoría informática desde una perspectiva muy amplia sin profundizar en temas más avanzados, como la eficiencia técnica. Los procesos informáticos y los archivos forman parte de los registros contables de las empresas y por ello, deben ser el objetivo de la auditoría.

El entorno informático en el que trabajan los auditores varía enormemente de un lugar a otro. Algunos sistemas son muy pequeños y forman parte de la organización general de la oficina; otros son grandes sistemas financieros independientes; otros son una mezcla de sistemas financieros y de gestión; otros tienen terminales de teleproceso

en departamentos usuarios; y por último, otros son una red de sistemas combinados. Las variaciones afectarán al enfoque que se haga de los trabajos de auditoría, aunque los objetivos de ésta pudieran ser similares en circunstancias distintas.

Para que el análisis sea eficaz y útil, el investigador deberá tener los conocimientos técnicos necesarios para comprender el tema que vaya a examinar.

La auditoría es una forma de asegurar la calidad de la información que contiene el sistema. La auditoría implica contar con un experto que no se encuentre involucrado en la puesta en operación y en el uso del sistema, para examinar la información, con el fin de establecer su relevancia. Si se encontrara o no información relevante, tal hallazgo deberá comunicarse a otros con el propósito de mejorar la relevancia de la información que les proporciona el sistema.

Generalmente existen para los sistemas de información, dos tipos de auditorías: interna y externa. El que ambas se necesiten para el sistema que se diseña dependerá del tipo de sistema. Las auditorías internas operan para la misma organización propietaria del sistema de información, mientras que en las auditorías externas se contratan auditores externos.

Básicamente se invita a los auditores externos cuando el sistema de información influye en los estados financieros del negocio. Los auditores

externos inspeccionan el sistema para asegurar la confiabilidad sobre los estados financieros que se producen. También deben traerse cuando algo fuera de lo ordinario está ocurriendo, se llegará a involucrar a los empleados de la compañía, tal como la sospecha de fraude en materia de computación o de peculado.

Los auditores internos estudian los controles utilizados por el sistema informático para asegurar que éste realiza lo que supuestamente debe de hacer. También examinan la operación de los controles de seguridad. Aunque trabajan dentro de la misma organización, los auditores internos no reportan a la gente responsable del sistema que auditan. El trabajo de los auditores internos, con frecuencia es de mayor profundidad que el de los auditores externos.

Diversos tipos de Auditoría y su relación con la Auditoría en Informática.

AUDITORIA INTERNA Y AUDITORIA CONTABLE/FINANCIERA.

El Boletín 3050 del Instituto Mexicano de Contadores Públicos 5, señala con respecto al control interno:

"El estudio y evaluación del control interno se efectúa con el objeto de cumplir con la norma de ejecución del trabajo que requiere que: el auditor debe efectuar un estudio y evaluación adecuados del control interno existente, que le sirva de base para determinar el grado de confianza que va a depositar en él, así mismo, que le permitan determinar la naturaleza, extensión y oportunidad que va a dar a los procedimientos de auditoría".

AUDITORIA ADMINISTRATIVA.

William P. Leonard define la auditoría administrativa como "un examen completo y constructivo de la estructura organizativa de una empresa, institución o departamento gubernamental; o de cualquier otra entidad y de sus métodos de control, medios de operación y empleo que dé a sus recursos humanos y materiales."⁶

6. William P. Leonard. Auditoría Administrativa.

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

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

La auditoría administrativa debe llevarse a cabo como parte de la auditoría del área de informática. Se ha de considerar dentro del programa de trabajo de auditoría en informática, tomando principios de la auditoría administrativa para aplicarlos al área de informática.

Se deberá evaluar el departamento de informática de acuerdo con:

- Su objetivo.
- Metas, planes, políticas y procedimientos.
- Organización.
- Estructura orgánica.
- Funciones.
- Niveles de autoridad y responsabilidad.

Es importante tener en cuenta los siguientes factores:

- Elemento humano.
- Organización (manual de organización).
- Integración.
- Dirección.
- Supervisión.
- Comunicación y coordinación.
- Delegación.
- Recursos materiales.
- Recursos técnicos.
- Recursos financieros.
- Control.

CAPITULO II

PLANEACION DE LA AUDITORIA.

Para hacer una adecuada planeación , hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo; con ello podremos determinar el número y características del personal de auditoría, las herramientas necesarias, el tiempo y el costo, así como definir los alcances de la auditoría para, en caso necesario, poder elaborar el contrato de servicios en caso de que sea externo de lo contrario no existirá dicho contrato.

La planeación de la auditoría tiene tres fases principales:

1o. Investigación de los aspectos generales y particulares de la empresa a examinar.

Comprende el estudio de todas aquellas cosas que hacen distintiva a la empresa que habremos de auditar, para poder con ese conocimiento genérico, decidir los aspectos específicos que deberá cubrir la planeación de dicha auditoría.

2o. Estudio y evaluación del control.

Desde el punto de vista técnico ésta es la fase de planeación más importante e implica el conocimiento formal de los métodos y rutinas que la empresa tiene establecidos para su operación y administración.

3o. Programación del trabajo de detalle específicamente aplicable.

Es decir formulación del programa de trabajo que indique cada uno de los trabajos específicos a realizar para lograr la obtención de evidencia suficiente y competente que apoye las conclusiones de la revisión, sobre las que se base la opinión final.

La planeación es fundamental, pues habrá que hacerla desde el punto de vista de 3 objetivos:

1o Evaluación administrativa del área de procesos electrónicos.

2o Evaluación de los sistemas y procedimientos.

3o Evaluación de los equipos de cómputo.

La evaluación administrativa del área de procesos electrónicos se estudiará al departamento de informática tanto a la gerencia como al personal subordinado.

Se considerará como está integrada dentro de la estructura orgánica, si existen organigramas, manuales, las políticas particulares y generales, sus objetivos, las funciones designadas, si existe la capacitación al personal que lo requiera, que motivación e incentivos se les otorga, etc. Esto y más se analizará en el capítulo III.

En la evaluación de los sistemas y procedimientos se estudiará que relación hay en el costo/beneficio, si realmente se obtiene la

información como es requerida por el usuario, que tan susceptible de modificarse y accesibles pueden ser los programas.

Si existe mantenimiento en que grado y como puede repercutir a la empresa y al departamento, la seguridad que para poder tener acceso a la información, técnicas y características de un requerimiento del usuario, la elaboración de un modelo conceptual y como puede ayudarnos, cómo saber del control de calidad de un programa, que beneficio nos trae tener una biblioteca de soporte de programas esto y más veremos con detalle en el capítulo IV.

La evaluación de los equipos de cómputo se analizará realizando pruebas para verificar que tan eficientes son los equipos pues se observará si es el adecuado, si hay seguridad para cualquier tipo de imprevisto, el mantenimiento que se les da, esto se ampliará con detalle en el capítulo V.

La planeación consiste, en fijar el curso concreto de acción que ha de seguirse, estableciendo los principios que habrán de orientarlo, la secuencia de operaciones para realizarlo y las determinaciones de tiempos y de números, necesarias para su realización.

Planear es hacer que ocurran cosas que, de otro modo, no habrían ocurrido (Goetz). Equivale a trazar los planos para fijar dentro de ellos nuestra futura acción.

Planear ¿cómo hacer? es tan importante, porque:

a) La eficiencia, no puede venir del acaso, de la improvisación.

7) Administración de Empresas. Agustín Reyes Ponce (Primera Parte).

b) Así como es la parte dinámica, lo central es dirigir, la mecánica el centro es planear, necesitamos primero hacer planes sobre la forma como esa acción habrá de coordinarse.

c) El objetivo sería infecundo, si los planes no lo detallaran, para que pueda ser realizado íntegra y eficazmente.

d) Todo control es imposible si no se compara con un plan previo. Sin planes, se trabaja a ciegas.

Los planes no deben hacerse con afirmaciones vagas y genéricas, sino con la mayor precisión posible, porque van a regir acciones concretas.

Las tareas y secuencias de pasos claves a realizarse para implantar los planes deben de ser determinados y comunicados; se deben identificar aquellas personas responsables de deberes específicos, y que tengan un conocimiento profundo acerca de lo que deben hacer.

Debe tenerse la seguridad de que los recursos, tanto humano como físicos, están o estarán disponibles cuando sea necesario para facilitar la implantación de planes.

Lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas y con base a esto planear el programa de trabajo, el cual

Lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas y con base a esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

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

Se debe de recopilar información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitudes de documentos; la finalidad es definir el objetivo y alcance del estudio, así como el programa detallado de la investigación.

Para poder analizar y dimensionar la estructura por auditar se debe solicitar:

a) A NIVEL ORGANIZACION TOTAL.

- Objetivos a largo o corto plazo.
- Manual de la organización.
- Políticas generales.

b) A NIVEL DEL AREA DE INFORMATICA.

- Objetivos a corto y largo plazo.
- Manual de organización.
- Manual de políticas y reglamentos.
- Manual de contingencias.
- Seguros.
- Contratos de mantenimiento.
- Bitácora de fallas.
- No. de personas y puestos en el área.
- Procedimientos administrativos del área.
- Presupuestos y costos del área.

c) RECURSOS MATERIALES Y TECNICOS.

- Solicitar documentos sobre los equipos, números de serie, localización y características.
- Fechas de instalación de los equipos y planes de instalación.
- Contratos vigentes de compra, renta y servicio de mantenimiento.
- Contratos de seguros.
- Convenios que se tienen con otras instalaciones.

- Configuración de los equipos y capacidades actuales y máximas.
- Políticas de operación.
- Políticas de uso de los equipos.

d) SISTEMAS.

- Descripción general de los sistemas instalados y de los que están por instalarse que contengan volúmenes de información.
- Manual de procedimientos de los sistemas.
- Diagrama de entrada, archivos y salida.
- Salidas.
- Fecha de instalación.
- Proyecto de desarrollo de nuevos sistemas. En el momento de hacer la planeación de la auditoría o bien su realización.

"Manual de Organización", es un documento detallado que contiene en forma ordenada y sistemática, información acerca de la organización de la empresa, generalmente contienen: objetivos generales de la organización, políticas generales, glosario de términos administrativos, nombres de áreas o departamentos y puestos, procedimientos de organización, responsabilidades de los altos niveles, funciones, cartas de organización descripción de puestos, descripción de actividades, introducción y objetivos del manual, e historia de la empresa.⁸

8). Munch Galindo y García Martínez. Editorial Trillas.

Problemas que pueden surgir en la recopilación de información.

a) SE SOLICITAN LA INFORMACION Y SE VE QUE :

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

b) SE TIENE LA INFORMACIÓN PERO:

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

El éxito del análisis crítico depende de las consideraciones siguientes:

- Estudiar los hechos y no opiniones.
- Investigar las causas, no los efectos.
- Atender razones no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y los datos recabados.

Una de las partes más importantes dentro de la planeación de la auditoría en información es el personal que deberá participar.

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervenga está debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Este es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual están presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

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

- Licenciados en informática.
- Conocimientos de administración.
- Experiencia en el área de informática.
- Experiencia en operación y análisis de sistemas.
- Conocimientos y experiencia en recursos humanos.
- Conocimientos de los sistemas más importantes.

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

Lo anterior no significa que una sola persona deberá contar con personal con conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características antes mencionadas.

Una vez planeada la forma de llevar a cabo la auditoría, se estará en posibilidad de presentar la carta convenio de servicios profesionales (en caso de auditores externos) y el plan de trabajo.

La carta convenio es un compromiso del auditor dirigida a su cliente para su confirmación de aceptación; en ella se especifican el objetivo y alcance de auditoría, las limitaciones y colaboración necesaria, el grado de responsabilidad y los informes que se han de entregar.

El hecho de contar con la información del avance nos permite revisar el trabajo elaborado por cualquiera de los asistentes.

Definición y objetivos del control interno.

"El control interno comprende el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la razonabilidad y confiabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la administración".⁹

Objetivos básicos Control Interno.

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

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

Se ha definido que los dos primeros objetivos abarcan el aspecto de controles internos contables y los dos últimos se refieren a controles internos administrativos.

9) Boletín 3050, Normas y procedimientos de Auditoría, Instituto Mexicano de Contadores Públicos.

Objetivos generales del Control Interno.

El control interno contable comprende el plan de organización y los procedimientos y registros que se refieren a la protección de los activos y a la confiabilidad de los registros financieros. Por lo tanto, el control interno contable está diseñado en función de los objetivos de la organización para ofrecer seguridad razonable de que: las operaciones se realizan de acuerdo con las normas y políticas señaladas por la administración.

Cuando hablamos de los objetivos de los controles contables internos podemos identificar dos niveles:

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

Los objetivos generales de control aplicables a todos los sistemas se desarrollan a partir de los objetivos básicos de control interno enumerados anteriormente, siendo más específicos para facilitar su aplicación. Los objetivos de control de ciclos se desarrollan a partir de los objetivos generales de control de sistemas, para que apliquen a las diferentes clases de transacciones agrupadas en un ciclo.

Los objetivos de control interno de sistemas se resumen a continuación.

Objetivos de Autorización.

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

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

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

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

Objetivos de Procesamiento y Clasificación de Transacciones.

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

Las transacciones deben clasificarse en forma tal que permitan al preparación de estados financieros en conformidad con los principios

de contabilidad generalmente aceptados y el criterio de la administración.

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

Objetivo de Salvaguarda Física.

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

Objetivo de Verificación y Evaluación.

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

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

En el primer caso se lleva el control interno por medio de la evaluación de una organización, utilizando la computadora como

herramienta que auxiliará en el logro de los objetivos del control interno, lo cual se puede hacer por medio de paquetes de auditoría. Y esto debe ser considerado como parte del control interno con informática.

En el segundo caso se lleva el control interno de informática. Es decir, como se señala en los objetivos del control interno, se deben proteger adecuadamente los activos de la organización por medio del control para que se obtenga la información en forma veraz, oportuna y confiable, se mejore la eficiencia de la operación de la organización mediante la informática y en la ejecución de las operaciones de informática se cumplan las políticas establecidas por la administración de todo ello debe ser considerado como control interno de informática.

Al estudiar los objetivos del control interno podemos ver en primer lugar que, aunque en auditoría en informática el objetivo es más amplio, se deben tener en cuenta los objetivos generales del control interno aplicables a todo ciclo de transacciones.

La auditoría en informática debe tener presentes los objetivos de autorización, procesamiento y clasificación de transacciones, así como los salvaguarda física, verificación y evaluación de los equipos y de la información. La diferencia entre los objetivos del control interno desde un punto de vista contable financiero es que, mientras éstos están enfocados a la evaluación de una organización mediante la revisión contable financiera y de otras operaciones, los objetivos del control

interno a informática están orientados a todos los sistemas en general, al equipo de cómputo y al departamento de informática, para lo cual se requieran conocimientos de contabilidad, finanzas, recursos humanos, administración, etc. y un conocimiento profundo y experiencia en informática.

Con base en los objetivos y responsabilidades del control interno podemos hacer dos preguntas:

De qué manera puede participar el personal de control interno en el diseño de los sistemas, qué conocimientos debe tener el personal de control interno para poder cumplir adecuadamente sus funciones dentro del área de informática.

Dependerán del nivel que tenga el control interno dentro de la organización; pero en el diseño general y detallado de los sistemas se debe incluir a personal de la contraloría interna, que habrá de tener conocimientos de informática; pero no se requerirá que sean especialistas ya que sólo intervendrán en el diseño general del sistema, diseño de controles, sistemas de seguridad, respaldo y confidencialidad del sistema, sistemas de verificación. Habrá de comprobar que las fórmulas de obtención del I.S.P.T., el cálculo del pago de I.M.S.S., S.A.R., INFONAVIT, etc. , pero no deben intervenir en la elaboración de los sistemas, bases de datos o programación. Y tendrán que comprobar que lo señalado en el diseño general sea igual a lo

obtenido en el momento de implantación, para que puedan dar su autorización a la corrida en paralelo.

El auditor interno, en el momento de que están elaborando los sistemas deben participar en las etapas siguientes:

1o Asegurarse de verificar que los requerimientos de seguridad y de auditoría sean incorporados, y participar en la revisión de puntos de verificación.

2o Revisar la aplicación de los sistemas y de control tanto con el usuario como en el centro de informática.

3o Verificar que las políticas de seguridad y los procedimientos estén incorporados al plan en caso de desastre.

4o Incorporar técnicas avanzadas de auditoría en los sistemas de cómputo.

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

El auditor interno desempeña una importante función al participar en los planes a largo plazo y en el diseño detallado de los sistemas y su implantación, de tal manera que se asegure de que los procedimientos

de auditoría y de seguridad sean incorporados a todas y cada una de las fases del sistema.

PROGRAMA DE TRABAJO

Última fase de la planeación, el programa de trabajo es representación física y la formalización de la planeación.

El programa de trabajo es la relación escrita y ordenada de los procedimientos de la auditoría, extensión y oportunidad de éstos, a aplicar en el trabajo específico.¹⁰

Un esquema donde se establecen: la secuencia de actividades específicas que habrán de realizarse para alcanzar los objetivos, y el tiempo requerido para efectuar cada una de las partes y todos aquellos eventos involucrados en su consecución.

Cada programa tiene una estructura propia y puede ser un fin en sí mismo, o bien, puede ser parte de una serie de actividades dentro de un programa más general.

La elaboración técnica de un programa debe apearse a :

- Identificar y determinar las actividades comprendidas.
- Ordenar cronológicamente la realización de las actividades.
- Interrelacionar las actividades. Es decir, determinar que actividad debe realizarse antes de otra, que actividades se dan simultáneamente y, por último, que actividades deben efectuarse posteriormente.

10). Elementos de Auditoría. Mendivil Escalante.

- Asignar a cada actividad la unidad de tiempo de su duración, así como los recursos necesarios.

Ventajas

- Permite visualizar el trabajo total y concluir sobre el tiempo probable de ejecución y consecuentemente, la fecha de entrega del trabajo.

- Al proporcionar un programa total del trabajo facilita el estudio inmediato de los problemas más importantes.

- Muestra el trabajo realizado y por realizar.

- Evita duplicidad de labores.

- Evita titubeos ya que señala claramente la acción concreta a desarrollar.

- Permite distribuir el trabajo y coordinarlo.

- En general, da seguridad al mostrar por escrito lo que se ha de hacer y elimina las eventualidades de la memoria.

El control interno tiene influencia directa en el programa de trabajo ya que frente a un control interno eficiente el Auditor puede reducir sus pruebas por la confianza que le merece; por lo contrario, cuando el control interno presenta serias deficiencias, las pruebas deben ser

ampliadas hasta un límite que permite juzgar el impacto total de los errores que un control interno así pudo permitir.

El resultado de la planeación se condensa en el programa de trabajo de auditoría, ya que para la revisión, es conveniente formular programas para uso y guía de los auditores, en la inteligencia de que sirvan no solo de guía y ayuda al grupo que efectúe la revisión, sino como también una salvaguarda de que no será omitido ningún detalle importante del trabajo. Desde luego que el programa no puede sustituir a la buena preparación y criterio del auditor, pues los procedimientos que deben seguirse en las revisiones no son siempre los mismos, ya que dependerán de las circunstancias particulares de cada empresa y en particular de la importancia y circunstancia del área de informática.

CAPITULO III

AUDITORIA DE LA FUNCION DE INFORMATICA

Una vez elaborada la planeación de la auditoría, la cual servirá como plan maestro de los tiempos, costos y prioridades, y como medio de control de la auditoría, se debe empezar la recolección de la información. La información nos servirá para determinar:

-Si las responsabilidades en la organización están definidas adecuadamente.

-Si la estructura organizacional está adecuada a las necesidades.

-Si el control organizacional es el adecuado.

-Si se tienen los objetivos y las políticas adecuadas.

-Si existe la documentación de las actividades, funciones y responsabilidades.

-Si el análisis y descripción de los puestos está de acuerdo con el personal que los ocupa.

-Si se cumplen los lineamientos organizacionales.

-Si los planes de trabajo concuerdan con los objetivos de la organización.

-Si se cuenta con los recursos humanos necesarios que garanticen la continuidad de la operación o se cuenta con lo indispensable.

-Si se evalúan los planes y se determinan las desviaciones.

Para que el control interno funcione en una empresa determinada, es necesario que su estructura organizacional esté diseñada para que quienes son responsables del establecimiento de los procedimientos de control y de su supervisión, tenga la autoridad necesaria para hacer cumplir sus objetivos; ésto es particularmente importante en el área de informática, ya que ocasionalmente estas funciones en las empresas serán nuevas o recientes y quizá no se les haya asignado un nivel adecuado en la estructura de la organización.

Como se mencionó en el capítulo anterior en la evaluación de los sistemas y procedimientos se estudiará que relación hay en el costo/beneficio, y nos hacemos la pregunta de ¿cómo podemos medirlo como auditor?.

Por lo general hay que determinar 2 factores: Productividad y % de Utilidad.

Para lo cual se consideran 3 partes esencialmente:

1o. Objetivos: los determinamos de acuerdo a las necesidades de información que ya se habían determinado. Hacerlos de acuerdo a las necesidades ya sean a corto, mediano o a largo plazo.

2o. ¿Qué necesitamos y cuánto nos costó o va a costar?

a) Determinar qué recursos vamos a necesitar ejem., tener el manual de procedimientos X , con el vamos a saber que gente se necesita, que hace, etc.

De acuerdo a lo anterior podemos saber ya que cantidad de equipo (software y hardware) se necesita.

b) Definir que cantidad de personal se va a necesitar para dar el servicio. Si hay un área de desarrollo de sistemas puede ser un analista y un programador. Si se usará paquetería, puede ser una persona con experiencia en su utilización.

c) Determinar el costo directo.

d) Determinar el costo de mantenimiento del equipo, por lo general el primero y segundo años no hay costos de mantenimiento (la garantía ampara los desperfectos).

e) Determinar no solo los costos de cada equipo sino el costo de la instalación (que incluye la instalación física y el servicio).

f) Realizar lista de proveedores para presentar cuáles son sus cotizaciones y tiempos de entrega. Plantear las diferentes alternativas, comparando proveedores.

3o. % de utilización del equipo de acuerdo a los objetivos a corto, mediano y largo plazo.

a) Cantidades: cuánto tiempo va a pasar para que esos 3 equipos estén utilizados toda la jornada normal de trabajo. Referente al uso físico.

b) C.P.U: Cómo se va a ir incrementando la cantidad de C.P.U. requerida para los procesos (alta al elaborar reportes). Plantear cómo va a ir incrementando la utilización de C.P.U. En captura es bajo, luego se va a ir incrementando. Por cada minuto de uso cuántos segundos de utilización de C.P.U. existen.

c) Almacenamiento: En cuánto tiempo considera que se va acabar la capacidad de almacenamiento que se tiene. ¿Cuánto tiempo se considera para que la capacidad instalada llegue a su máximo o límite. Video, memoria, disco duro, etc. Normalmente se busca cuándo va a llegar al 80%.

Esto nos beneficia para justificar que el equipo va a ser realmente utilizado.

¿Cómo se va a notar el aumento en las utilidades ? ¿Cómo hacer tangibles los beneficios?

Utilidades se expresa en \$ y Productividad en %.

Primero se debe ver la productividad. La relación de productividad debe ser positiva.

Después de determinar los porcentajes de utilidad se convierten a pesos \$ (utilidades). Utilidades pueden resultar de:

- * Ahorros en sueldos.
- * Multas y recargos,

* Honorarios de servicios externos.

* Ahorro en provisiones.

Debe incluirse también el costo de capacitación.

Controles Generales.

Los controles generales del proceso electrónico de datos se enfocan a la organización general del departamento y a las funciones de quienes intervienen en el desarrollo de sistemas; esto es en el medio ambiente en el que se desarrollan los sistemas.

1o Pre-instalación.

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

2o Organización del departamento de informática.

Comprende la correcta estructura organizacional del departamento, principalmente la adecuada segregación de labores, la definición de políticas, funciones y responsabilidades, así como la asignación de personal competente.

3o Control del desarrollo de sistemas.

Se debe contar con estudios preliminares que justifiquen las aplicaciones, así como con definición de los estándares para el diseño, programación, prueba y mantenimiento de los sistemas. Estos estudios y los estándares definidos por la empresa deben quedar documentados adecuadamente.

Al desarrollar nuevos sistemas puede ser necesario llevar en paralelo, por tiempo necesario, el sistema anterior y el nuevo.

Es necesario que en la definición de los estándares para el desarrollo de sistemas, se incluyan los procedimientos que aseguren que el sistema a desarrollar ha sido autorizado por un funcionario responsable y, además, que en el propio desarrollo exista una intervención activa del que va a ser usuario del sistema y de quien lo va auditar, esto último con el objeto de establecer desde esta etapa, los controles necesarios y las pistas de auditoría. En la definición de estándares, también deben incluirse los procedimientos de autorización de cambios.

4o Control de la documentación.

Necesidad de que todos los programas, la operación y los procedimientos relativos estén adecuadamente documentados y actualizados. Es conveniente que se tenga copia-respaldo actualizada de esta documentación fuera de las instalaciones del centro de cómputo, así como la historia de los cambios efectuados.

5o Control de la operación.

Comprende la creación de un medio ambiente que garantice efectividad en la producción de la sección de operaciones y proporcione la seguridad física suficiente sobre los registros que se mantienen en el centro de cómputo, así como el establecimiento de controles adecuados que eviten el acceso de personal no autorizado; esto es especialmente crítico cuando existe teleproceso.

Es muy importante también contar con una razonable seguridad contra la destrucción accidental de los registros durante el proceso y asegurar la continuidad de la operación y, en su caso, la receptora de datos; asimismo, prevenir y detectar la manipulación fraudulenta de datos durante los procesos por el personal del departamento y prevenir el mal uso de la información. Con el fin de no entorpecer los procesos cuando ocurran rupturas importantes en el computador, se deberá contar con equipos de respaldo para ser utilizados en esos casos. Asimismo llevar a cabo simulacros con dichos equipos para asegurar que no ha habido cambios que imposibiliten la utilización oportuna de dichos equipos de respaldo.

Evaluación de la Estructura Orgánica.

Para lograr el objetivo de ésta evaluación se deberá solicitar el manual de organización de la dirección, el deberá comprender como mínimo.

- Organigrama con jerarquías.
- Funciones.
- Objetivos y políticas.
- Análisis, descripción y evaluación de puestos.
- Manual de normas y procedimientos.
- Instructivos de trabajo o guías de actividad.
- Objetivos de la dirección.
- Políticas y normas de la dirección.

El director de informática y aquellas personas que tengan un cargo gerencial deben llenar los cuestionarios sobre estructura orgánica, funciones y políticas; a continuación se presenta un ejemplo de dicho cuestionario:

- 1o ¿ Qué se espera del departamento de informática ?
- 2o ¿ Qué función tiene el departamento ?
- 3o ¿ Qué objetivos hay a corto, mediano y largo plazo ?
- 4o ¿ Se están llevando a cabo dichos objetivos ?
- 5o ¿ Existe un manual específico de políticas para el departamento ?
- 6o ¿Qué responsabilidades tiene el personal con relación a la dirección ?

7o ¿ Cuando se adquiere material y/o equipo se realizan pruebas que demuestre lo que se esperaba ?

8o ¿ Se cuenta con equipo de seguridad en el departamento ?

9o ¿ Qué relación tiene el departamento de informática con respecto a los demás ?

10o ¿ Cada cuándo se capacita al personal del departamento ?

11o ¿ Existe un manual de organización ?

12o ¿ Los manuales del usuario son entendibles y se entregan con oportunidad ?

El "manual de usuario " es un instructivo para instalar, operar y mantener el sistema ó paquete de programación. Dependiendo de la complejidad del sistema y de la extensión de su documentación, el manual de usuario podrá ser presentado en un solo documento, ó bien, como un conjunto de guías que tratan en forma independiente los aspectos básicos de instalación, operación y mantenimiento.

El cuestionario se presenta con el objeto de poder dar a conocer la organización del departamento de informática y su dependencia dentro de la organización.

El departamento de informática básicamente puede estar dentro de algunos de los casos siguientes:

a) Depende de alguna dirección o gerencia la cual, normalmente, es la dirección de finanzas. Esto se debe a que inicialmente informática

procesaba principalmente sistemas de tipo contable, financiero o administrativo.

La ventaja que tiene es que no se crea una estructura adicional para el área de informática y permite que el usuario principal tenga un mayor control sobre sus sistemas.

La desventaja principal es que los otros usuarios son considerados como secundarios y normalmente no se les da la importancia y prioridad requerida; otra desventaja es que, como la información es poder, a veces hace que un área tenga un mayor poder.

b) La dirección de informática depende de la gerencia general; esto puede ser en línea o en forma de asesoría.

La ventaja de alguna de estas organizaciones es que el director de informática podrá tener un nivel adecuado dentro de la organización, lo cual le permitirá lograr una mejor comunicación con los departamentos usuarios y por lo tanto, proporcionarles un mejor servicio y asignar las prioridades de acuerdo con los lineamientos dados por la gerencia general.

La desventaja es que aumentan los niveles de la organización, lo que elevará el costo de utilización de los sistemas de cómputo.

c) La tercera posibilidad es para estructuras muy grandes en la que hay bases de datos, redes.

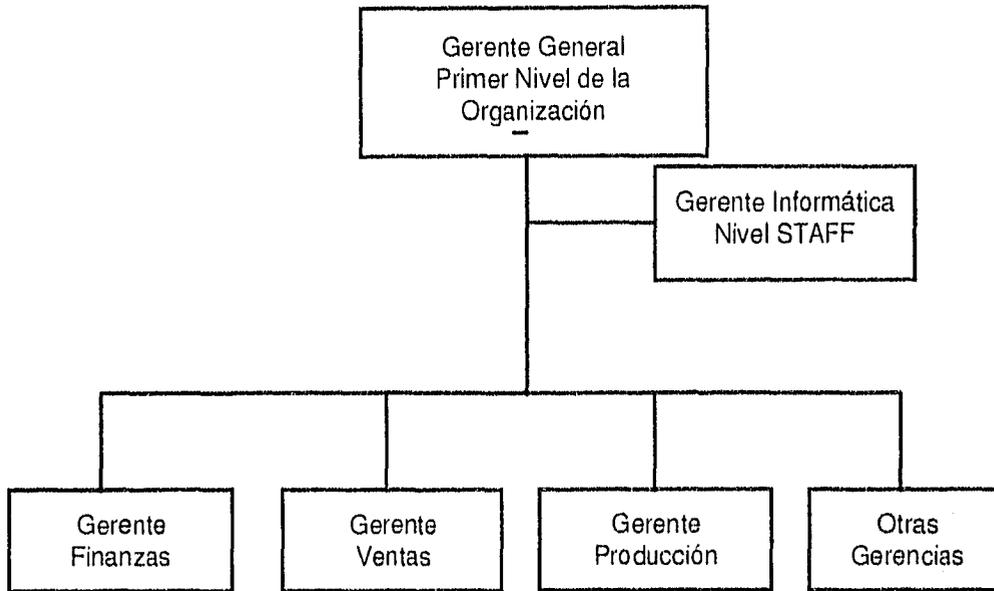
La dirección de informática depende de la gerencia general, o de departamentos de informática dentro de las demás gerencias, las cuales reciben todas las normas, políticas, procedimientos y estándares de la dirección de informática, aunque funcionalmente dependa de la gerencia a la cual están adscritas. Son controladas en cuanto a sus funciones y equipo en forma centralizada por la dirección de informática.

Deben estar perfectamente definidas las funciones, organización y políticas de los departamentos para evitar la duplicidad de mando y el que en dos lugares diferentes se estén desarrollando los mismos sistemas o bien que sólo en un lugar se programe, y no se permita usar los equipos para programar en otro lugar que no sea la dirección de informática.

La ventaja principal de la organización consiste en que se puede tener centralizada la información (base de datos) y descentralizados los equipos; pero se debe tener una adecuada coordinación entre la dirección de informática y los departamentos de informática de las áreas usuarias para evitar duplicar esfuerzos o duplicidad de mando.

Al analizar las organizaciones debemos tener muy en cuenta si están definidas las funciones y la forma de evaluar a las personas que ingresan a los diferentes niveles de la organización.

**LA GERENCIA DE INFORMATICA ESTA DEPENDIENDO
DE LA GERENCIA GENERAL COMO STAFF**



CAPITULO IV

EVALUACION DE LOS SISTEMAS.

La elaboración de sistemas debe ser evaluada con mucho detalle, para lo cual se debe revisar si existen realmente sistemas entrelazados como un todo o bien si existen programas aislados.

El plan estratégico deberá establecer los servicios que se presentarán en un futuro contestando preguntas como las siguientes:

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

La estrategia de desarrollo deberá establecer las nuevas aplicaciones y recursos que proporcionará la dirección de informática y la arquitectura en que estarán fundamentados.

- ¿ Qué aplicaciones serán desarrolladas y cuándo ?.
- ¿ Qué tipo de archivos se desarrollarán y cuándo ?.
- ¿ Qué bases de datos serán desarrolladas y cuándo ?.
- ¿ Qué lenguajes se utilizarán y en qué software ?.
- ¿ Qué tecnología será utilizada y cuándo se implementará ?.
- ¿ Cuántos recursos se requerirán aproximadamente ?.

-¿Cuál es aproximadamente el monto de la inversión en hardware y software ?.

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

Para identificar los problemas de los sistemas primero debemos detectar los síntomas, los cuales son un reflejo de la problemática y después de analizarlos podremos definir y detectar las causas, parte medular de la auditoría.

Debemos aprender a reunir todos los síntomas y a distinguirlos antes de señalar las causas, evitando tornar los síntomas como causas dejando fuera todo lo que es rumores sin fundamento.

Los sistemas se deben evaluar de acuerdo con el ciclo de vida que normalmente siguen: requerimientos del usuario, estudio de factibilidad, diseño general, análisis, diseño lógico, desarrollo físico, pruebas, implementación, evaluación, modificaciones, instalación mejoras. Y se vuelve nuevamente al ciclo inicial, el cual a su vez debe comenzar con el de factibilidad.

La primera etapa a evaluar el sistema es el estudio de factibilidad, el cual debe analizar si el sistema es susceptible de realizarse, cuál es su relación costo/beneficio y si es favorable.

Se deberá solicitar éste estudio de los diferentes sistemas que se encuentren en operación, así como los que estén en la fase de análisis para evaluar si se considera la disponibilidad y características del equipo, los sistemas operativos y lenguajes disponibles, las necesidades de los usuarios, las formas de utilización de los sistemas, el costo y los beneficios que reportará el sistema, el efecto que producirá en quienes lo usarán y el efecto que éstos tendrán sobre el sistema, y la congruencia de los diferentes sistemas.

El costo de un sistema se debe considerar, con una exactitud razonable, el costo de los programas, el uso de los equipos (compiladores, programas, pruebas, paralelos) tiempo, personal y operación, cosa que en la práctica son costos directos, indirectos y de operación.

Los beneficios que justifiquen el desarrollo de un sistema pueden ser el ahorro en los costos de operación, la reducción del tiempo de proceso de un sistema, mayor exactitud, mejor servicio, una mejoría en los procedimientos de control, mayor confiabilidad y seguridad.

Entre los problemas más comunes en los sistemas están los siguientes:

1o Falta de estándares en el desarrollo , en el análisis y en la programación.

2o Falta de participación y de revisión por parte de la alta gerencia.

3o Falta de participación de los usuarios.

4o Inadecuada especificación del sistema al momento de hacer el diseño detallado.

5o Deficiente análisis costo/beneficio.

6o Nueva tecnología no usada o usada incorrectamente.

7o Diseño deficiente.

8o Control débil o falta de control sobre las fases de elaboración del sistema y sobre el sistema en sí.

9o Problemas de auditoría.

10o Documentación inadecuada o inexistente.

11o Dificultad de dar mantenimiento al sistema, principalmente por falta de documentación o excesivos cambios y modificaciones hechos al programa.

12o Inadecuados procedimientos de seguridad, de recuperación y de archivos.

13o Procedimientos incorrectos o no autorizados.

14o Inexperiencia por parte del personal de análisis y el de programación.

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

La auditoría en informática debe evaluar los documentos y registros usados en la elaboración del sistema, así como todas las salidas y reportes, la descripción de las actividades de flujo de la información de los procedimientos, los archivos almacenados, su uso y su relación con otros archivos y sistemas, su frecuencia de acceso, su conservación, su seguridad y control, la documentación propuesta, las entradas y salidas del sistema y los documentos fuentes a usarse.

También se deberán analizar las especificaciones del sistema, estudiar la participación que tuvo el usuario en la identificación del nuevo sistema, la participación de auditoría interna en el diseño de los controles y la determinación de los procedimientos de operación y decisión.

Al tener el análisis del diseño lógico del sistema debemos compararlo con lo que realmente se está obteniendo.

Los puntos a evaluar son:

- Entradas.
- Salidas.
- Procesos.
- Especificaciones de datos.
- Especificaciones de proceso.
- Métodos de acceso.
- Operaciones.
- Manipulaciones de datos.
- Proceso lógico necesario para producir informes.
- Identificación de archivos.
- Sistemas de seguridad y control.
- Responsables y número de usuarios.

En ésta etapa (evaluación del desarrollo del sistema) se deberán auditar los programas, su diseño, el lenguaje utilizado, interconexión entre los programas y características del hardware empleado para el desarrollo del sistema.

El proceso de planeación de sistemas debe definir la red óptima de comunicaciones, recordando que el plan de aplicaciones proporciona información de la ubicación planeada de las terminales, los tipos de mensajes requeridos, el tráfico esperado en las líneas de comunicación y otros factores que afectan el diseño.

Las características que deben evaluarse en los sistemas son:

- Dinámicos (susceptibles de modificarse)
- Estructurados (las interacciones de sus componentes o subsistemas deben actuar como un todo).
- Integrados (un sólo objetivo). En él habrá sistemas que puedan ser interrelacionados y no programas aislados.
- Accesibles (que estén disponibles).
- Necesarios (que se pruebe su utilización).
- Comprensibles (que contengan todos los atributos)
- Oportunidades (que está la información en el momento que se requiere)
- Funcionales (que proporcionen la información adecuada a cada nivel).
- Estándar (que la información tenga la misma interpretación en los distintos niveles).
- Modulares (facilidad de ser expandidos o reducidos).
- Jerárquicos (por niveles funcionales).
- Seguros (que sólo las personas autorizadas tengan acceso).
- Inicios (que no se duplique la información).

Debido a las características propias del análisis y la programación, es muy frecuente que la implantación de los sistemas se retrase y se llegue a suceder que una persona lleva trabajando varios años dentro de un sistema o bien que se presenten irregularidades en las que los programadores se ponen a realizar actividades ajenas a la dirección de informática. Para poder controlar

el avance de los sistemas, ya que ésta es una actividad intelectual de difícil evaluación, se recomienda que se utilice la técnica de administración por proyectos para su control adecuado.

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

Las revisiones se efectúan en forma paralela desde el análisis hasta la programación y sus objetivos son los siguientes:

1o ETAPA DE ANALISIS. Identificar inexactitudes, ambigüedades y omisiones en las especificaciones.

2o ETAPA DE DISEÑO. Descubrir errores debilidades omisiones antes de iniciar la codificación.

3o ETAPA DE PROGRAMACION. Buscar la claridad, modularidad y verificar con base en las especificaciones.

Esta actividad es muy importante ya que el costo de corregir errores es directamente proporcional al momento que se detectan; si se descubren en el momento de programación será más alto el costo que si se detectan en la etapa del análisis.

El mantenimiento excesivo es consecuencia de falta de planeación y control del desarrollo de sistemas; la planeación debe contemplar los recursos disponibles y técnicas apropiadas de desarrollo.

Mantenimiento. Dentro del campo de programación es necesario aclarar el término mantenimiento, que generalmente se utiliza para describir todos aquellos cambios hechos a la programación después de su primera instalación. Por ello difiere significativamente de su concepto general, que describe la restauración de un sistema o componente a su estado original. El deterioro que ha ocurrido en los diferentes sistemas físicos como un resultado del uso o del paso del tiempo se corrige reparando o sustituyendo los elementos deteriorados. La programación no se deteriora espontáneamente por una interacción con el medio, no cambia a menos de que alguien la haga cambiar como resultado de un deseo de eliminar errores o de un funcionamiento poco adecuado ó restringido.

El control por su parte debe tener como soporte el establecimiento de normas de desarrollo que han de ser verificadas continuamente en todas las etapas del desarrollo de un sistema. Estas normas no pueden estar aisladas, primero, del contexto particular de la dirección de informática (ambiente) y, segundo, de los lineamientos generales de la organización, para lo cual es necesario contar con personal en desarrollo que posea suficiente experiencia en el establecimiento de normas de desarrollo de sistemas. Estas mismas características deben existir en el personal de auditoría.

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

Para verificar si existe esta situación, se debe pedir a los analistas y a los programadores las actividades que están desarrollando en el momento de la auditoría y evaluar si están efectuando actividades de mantenimiento o de realización de nuevos proyectos. En ambos casos se deberá evaluar el tiempo que llevan dentro del mismo sistema, la prioridad que se le asignó y cómo está en el tiempo real en relación al tiempo estimado en el plan maestro.

El que los analistas, los programadores o unos y otros tengan acceso en todo momento a los sistemas en operación puede ser un grave problema y ocasionar fallas de seguridad.

El impacto en el rendimiento de un sistema de cómputo debido a cambios trascendentales en el sistema operativo o en el equipo puede ser determinado por medio de un paquete de pruebas que haya sido elaborado para este fin en la dirección de informática. Es conveniente solicitar pruebas y comparaciones entre equipos para evaluar la situación del equipo y del software en relación a otros que se encuentran en el mercado.

Técnicas de definición de Requerimientos.

Describen cómo el empleo de modelos conceptuales ayuda a establecer requerimientos con las características ya citadas, la estructura que debe tener el documento de requerimientos y las tendencias que se observan en el desarrollo de herramientas automáticas que facilitan el establecimiento de los requerimientos de un programa.

Son cinco las principales características que una especificación de requerimientos debe poseer:

1o Intangible. Debe indicar claramente las tareas que el sistema de cómputo propuesto realizará, incluyendo la interacción con otros sistemas (humanos y equipo), en términos que el usuario, el analista de sistema y el especialista en cómputo, puedan comprender.

2o Preciso y formal. Debe definir el sistema propuesto de manera precisa y formal, para así verificar la correcta realización del producto una vez que éste haya sido terminado.

3o Completo. Debe describir el sistema en forma completa para propósitos de desarrollo, cubriendo todos aquellos aspectos que no deben dejarse a la libre elección del diseñador.

Por estas razones se dice, que una especificación de requerimientos debe ser intangible, formal y completa. A estas tres características es necesario agregar dos adicionales:

4o Actualizable y modificable. El documento de especificación debe ser estructurado, a manera de permitir el uso de las partes terminadas mientras se desarrollan otras. Se deberá procurar minimizar el impacto de modificaciones sobre el documento.

5o Mantenable. El documento debe ser mantenible. En el caso de sistemas complejos, cuyos documentos contienen más de 1000 páginas, el proceso de mantener la documentación actualizada ante cambios que ocurren durante el desarrollo del sistema o durante su operación, se convierte en una actividad crítica. Es por esto, que otra de las principales características del documento debe ser su mantenibilidad.

Entre las principales deficiencias que con mayor frecuencia se presentan en documentos típicos de especificaciones se encuentran las siguientes:

- 1o Especificaciones infactibles o erróneas.
- 2o Omisión de información clave.
- 3o Información dudosa.
- 4o Pobre presentación.
- 5o Información obsoleta.

El empleo de una buena metodología durante la etapa de "especificación", así como la adopción de una norma adecuada a la naturaleza del proyecto, ayuda a eliminar las deficiencias mencionadas.

La metodología de especificación puede definirse como un conjunto de técnicas apropiadas para la adquisición, análisis y presentación de información acerca de un sistema. Esta metodología debe cubrir los siguientes aspectos:

1o Identificación de los pasos que se deben seguir durante la fase de definición de requerimientos.

2o La forma de adquirir, analizar y verificar la información requerida sobre el sistema.

3o La forma de presentar información a través de prosa, notaciones y lenguajes especializados.

La norma de especificación de requerimientos puede definirse como un conjunto de reglas que gobiernan la elaboración del documento y definen el criterio de aprobación de los documentos terminados.

La norma debe establecer la terminología, el grado de detalle, la estructura y el tipo de lenguaje permitido en el documento, así como definir el procedimiento para actualizar las partes terminadas. Es a través de la norma que se pueda lograr un producto actualizado con buena presentación.

A continuación se tratan los aspectos principales de la metodología de especificación.

Modelos Conceptuales.

Un modelo conceptual de un sistema es un conjunto de información que se colecta con el propósito de estudiarlo. Puesto que el propósito del estudio determina la naturaleza de la información que se colecta, no existe un modelo único por sistema. Se puede elaborar diferentes modelos de un mismo sistema con el fin de estudiarlo desde distintos puntos de vista.

En términos generales, todo modelo conceptual de un sistema comprende los siguientes conceptos y las relaciones que existen entre ellos:

1o Entidades y Atributos. El término entidad se utiliza como sinónimo de componente en un sistema. El término atributo representa una propiedad o característica de entidades. Una entidad puede poseer varios atributos.

2o Proceso. Proceso es sinónimo de toda acción que origina cambios en el sistema. Cualquier fenómeno que presenta una continua modificación al través del tiempo, la cual se traduce en operación permanente; una relación cambiante, cuyos componentes o partes interaccionan y se influyen recíprocamente.

3o Frontera y Ambiente. La frontera separa al sistema del ambiente que le rodea. La interacción entre el sistema y su ambiente ocurre a través de la frontera. Pueden existir procesos dentro del sistema que originan también cambios en el exterior y viceversa.

El formalismo de crear el modelo conceptual de un sistema impone una disciplina en la manera de adquirir y analizar información relativa al sistema. Esta disciplina permite identificar los aspectos oscuros o desconocidos del sistema.

El modelo conceptual ayuda a entender la problemática del sistema y permite comprender las necesidades del usuario.

El estudio del sistema, a través de su modelo conceptual, permite interpretar los objetivos que el usuario establece para el proyecto y es una herramienta necesaria para el análisis de su factibilidad.

El trabajo de crear un modelo conceptual consiste en establecer su estructura y suministrar sus datos. Estableciendo su estructura se dan a conocer sus entidades, atributos procesos, frontera y ambiente. Suministrando sus datos se dan a conocer los valores de sus atributos y las relaciones que pueden ocurrir entre estímulos, procesos y respuestas.

Los conceptos más utilizados para reducir complejidad son:

1o Abstracción. Estudia el sistema en etapas sucesivas, incorporando mayor detalle y reduciendo el nivel de abstracción en cada nueva etapa.

2o Participación. Consiste en descomponer el sistema en un conjunto de subsistemas, permitiendo el estudio del sistema completo

a través del estudio de todas sus partes y de las interacciones que ocurren entre ellas.

3o Relevancia. Incluye el modelo únicamente aquellos aspectos del sistema que son relevantes para los objetivos del estudio deseado.

4o Compactación. Permite agrupar entidades del sistema con atributos similares para formar entidades de carácter más general y reducir el número de entidades en el modelo.

5o Proyección. Consiste en estudiar un sistema desde distintos puntos de vista, dando origen a un modelo conceptual del sistema completo.

Si los modelos conceptuales constituyen una herramienta útil para que los analistas estudien y comprendan las características de un sistema, es evidente que también apoyan a los analistas al describir las características del sistema a otras personas, en particular, a aquellos que diseñarán y desarrollarán los programas del sistema.

Formalismo y Lenguajes de Especificación.

La forma tradicional de especificar requerimientos consiste en describir las características del sistema a desarrollar en un lenguaje natural, apoyándose en el uso de diagramas de proceso y de flujo de información.

Se ha generado, una tendencia al uso de lenguajes formales de especificación, dotados de una sintaxis y una semántica bien definida, que con su notación precisa y restrictiva elimina ambigüedades y permiten la verificación automática de consistencia en las especificaciones. El gran beneficio que aporta el formalismo de estos lenguajes es el uso de herramientas automáticas para almacenar y procesar la información clave de las especificaciones. Las herramientas automáticas son utilizadas para las siguientes funciones:

1o. Asegurara consistencia en las especificaciones, verificando, por ejemplo, que no exista tarea alguna cuya información de entrada no sea generada por otra tarea o por el ambiente.

2o Asegurar la integridad del diseño, verificando que todos los requerimientos hayan sido considerados.

3o Asegurar la correcta realización del sistema, generando automáticamente casos de prueba que permitan verificar la satisfacción de requerimientos.

Son muchos los lenguajes de especificación que se han desarrollado y muy variados los enfoques utilizados en su diseño.

La desventaja de un formalismo acentuado es la dificultad que se impone a la comunicación entre personal de distintas disciplinas. El formalismo reduce legibilidad en favor de precisión.

La tendencia actual en el desarrollo de especificaciones de requerimientos pretende lograr un compromiso entre un formalismo acentuado, que es difícil de usar y leer, y un lenguaje natural que presenta confusión e inconsistencia. Se pretende que la notación sea rigurosa para que permita el procesamiento automático de especificaciones y a la vez, sea suficientemente legible para permitir la comunicación entre usuario, analista y diseñador.

Diseño de la Arquitectura.

La parte medular del diseño de la arquitectura es un diagrama de flujo del sistema que indica por medio de gráficas, la interacción de diferentes partes de un sistema: la base de datos y sus archivos, los programas y los operadores.

El diseño de la arquitectura define:

- 1o Los conjuntos de información.
- 2o Los procesos o programas a desarrollar.
- 3o El comportamiento dinámico.
- 4o Las interacciones organizacionales.
- 5o Las responsabilidades.

Los conjuntos de información se clasifican en tres tipos:

1o Entrada. Los conjuntos de datos de entrada son todos aquellos elementos de información necesarios para la correcta operación de la programación, y que usualmente se captura a través de los diferentes dispositivos de lectura de los sistemas de cómputo, tales como

unidades de cinta magnética, terminales de video, lectoras de tarjetas, etc.

2o Salida. Los conjuntos de datos de salida incluyen todo tipo de información producida por el sistema como pueden ser cheques impresos, reportes, sobres con direcciones, gráficas, etc.

3o Base de Datos. La base de datos concentra toda la información que es producida internamente, mantenida y usada por el sistema. Su diseño adecuado es uno de los factores más importantes en el desarrollo de un sistema de cómputo.

Identificación de programas.

La siguiente actividad en el desarrollo de la arquitectura de un sistema consiste en identificar el número de programas o procesos a desarrollar y las interfases entre ellos. El resultado de esta actividad se puede documentar utilizando diagramas de flujo de información, que son gráficas que, para cada programa, especifican los conjuntos de información con que interactúa.

El Comportamiento Dinámico del Sistema.

La definición del comportamiento dinámico consiste en especificar los eventos y condiciones que afectan al sistema. Los eventos describen hechos que pueden ocurrir durante la operación del sistema.

Las Interacciones Organizacionales.

Las interacciones organizacionales con el sistema describen las responsabilidades del medio ambiente con respecto al sistema. Se define quién proporciona la información de entrada y en dónde se deposita la salida del sistema.

Las Responsabilidades.

Finalmente, la arquitectura de un sistema deberá incluir la definición de los responsables de diversas actividades del diseño, los nombres de las personas y su responsabilidad.

Diagrama de Estructura.

Para cada programa identificado al establecer la arquitectura se deberá construir un diagrama de estructura, que representa la subdivisión jerárquica y funcional de un programa.

Presentaremos una serie de criterios para evaluar si un diagrama de estructura ha sido diseñado correctamente. Estos criterios son los siguientes:

1o Tamaño. Dependiendo del lenguaje de programación que se esté utilizando.

2o Acoplamiento. Es la medida de interdependencia entre módulos

3o Cohesión. El concepto de acoplamiento ayuda a evaluar las interfases entre módulos y la forma como éstas afectan el mantenimiento y la reutilización de los mismos.

4o Parsimonia. Utilizado para evaluar el diseño de un diagrama de estructura, se emplea para evitar la concepción de módulos de propósito general. Las funciones de los módulos deberán asociarse exclusivamente al cumplimiento de los requerimientos del programa de cómputo.

CONTROL DE CALIDAD.

El objetivo del "Control de Calidad" es garantizar que todos los productos de programación satisfagan los requerimientos que han sido acordados. El control de calidad, en el contexto de desarrollo de programación, es un proceso muy complejo debido a la característica intangible de los programas de computadora, la dificultad de especificar adecuadamente los requerimientos y la ambigüedad inherente de las especificaciones y otra documentación de programación.

El grupo encargado de controlar la calidad de la programación debe recibir información de los productos elaborados durante cada una de las distintas fases y etapas en el desarrollo de programación. Un resumen de los diferentes productos generados durante el proceso de programación, que deberán ser auditados.

Norma de Especificación de Requerimientos.

La norma de requerimientos es un conjunto de reglas establecidas por el líder analista de un proyecto, que sirve para guiar y controlar el desarrollo de especificación de los requerimientos.

Las bases para dotar al requerimiento del programa de computadora con las características deseadas, se deben sentar estableciendo la norma antes de iniciar el desarrollo de la especificación de requerimientos. La norma es particularmente necesaria en proyectos

de gran escala, en donde el análisis y el desarrollo de los requerimientos es realizado por un número elevado de analistas. Los distintos hábitos de redacción, presentación de ideas y organización de documentación, de no ser normalizados, pueden dar origen a una especificación de requerimientos mal presentado, difícil de mantener, poco claro y con distintos grados de detalle.

La norma, en general, debe ser establecida para cada caso, considerando las condiciones particulares que influyen en su desarrollo, como la naturaleza técnica del proyecto, el entrenamiento del personal secretarial, el número de analistas, las facilidades de procesamiento de textos, etc.

Criterio de Revisión y Aceptación de la Especificación de Requerimientos.

La norma deberá definir quien o quienes revisarán y aprobarán el documento de especificación de requerimientos y precisar las técnicas que se emplearán durante los procesos de revisión.

Herramientas de Elaboración y Almacenamiento de la Especificación de Requerimientos.

La norma deberá definir el medio que será utilizado para producir el documento de especificación de requerimientos (por ejemplo, procesador de textos, paquete de soporte de desarrollo de sistemas, máquina de escribir convencional, etc.). Es también recomendable definir el medio que se empleará para almacenar la información, que puede ser disco magnético o expedientes, así como la forma en que se podrá obtener la información almacenada citando las convenciones o reglas para nombrar los expedientes o archivos a fin de facilitar la consulta de material de capítulos y secciones de la especificación de requerimientos durante su desarrollo y edición.

Sintáxis y Palabras Reservadas.

La fácil identificación de requerimientos a lo largo de la especificación de requerimientos es necesaria. La facilidad para localizar con rapidez los requerimientos a lo largo del texto se puede lograr utilizando palabras de uso restringido en combinación con una sintáxis bien definida.

Normas de codificación.

Los estándares o normas de programación son un conjunto de reglas de estilo que permiten que los programas sean fáciles de leer, revisar, modificar y por lo consiguiente mantener.

Este conjunto de normas generales de programación también tiene como objetivo unificar el estilo de programación, sin limitar la creatividad del programador. Se entiende por estilo, la selección adecuada de hábitos de programación que favorecen la claridad y eficiencia del programa.

El empleo unificado de estos hábitos coadyuva a la producción de buenos programas, cuya principal característica desde luego es que deben trabajar. La velocidad, la utilización del tiempo de máquina, el número de líneas de código y otras variables cuantificables no tienen significado si el programa no trabaja. Con relación a esas características puede afirmarse que:

1o El programa debe ser correcto antes de ser rápido.

2o Debe ser factible antes de ser rápido.

3o Debe tener bajos costos de desarrollo.

4o Debe tener bajos costos de prueba.

5o Debe tener costos mínimos de mantenimiento. Es de advertirse, que las organizaciones que emplean masivamente procesamiento de información gastan entre el 50 y 90%¹¹ de su presupuesto anual en el mantenimiento de sistemas existentes.

11) Desarrollo y Administración de Programas de Computadora (sep/85).

6o Debe ser fácilmente modificable. Dentro del dinámico ambiente de una empresa moderna, los requerimientos de los programas cambian continuamente hasta el módulo más pequeño. Un buen programa deberá estar diseñado tomando en cuenta las eventuales necesidades de revisión y cambio.

7o Debe tener un diseño poco complicado. Siempre deberá diseñarse un programa con la idea de que alguna otra persona lo va a mantener.

Herramientas Automáticas.

Los sistemas de programación han alcanzado proporciones normas, tanto en tamaño como en complejidad. El control de calidad en la programación es un proceso complejo, dada la intangibilidad de los programas de computadora y la dificultad de establecer bases con las cuales compararlos. Por ello para controlar adecuadamente la calidad de estos sistemas difíciles de coordinar, es necesario emplear un gran número de recursos humanos, lo cual resulta muy costoso y no particularmente eficiente. Para mejorar esta situación se han desarrollado herramientas automáticas, que no solamente facilitan la labor descrita, sino que aseguran que los distintos programas desarrollados sean homogéneos. El empleo de herramientas automáticas provee los siguientes beneficios:

1o Permite incrementar el volumen de pruebas a través de su automatización.

2o Permite aplicar con mayor vigor el proceso de auditoría.

3o Tiene mayor aceptación que métodos manuales por parte de los integrantes del grupo.

4o Reduce el costo de control de calidad.

Se describen dos herramientas automáticas que asisten al desarrollo de programación, concretamente el la audición estática del código fuente y en el registro y mantenimiento de programas. Estas herramientas son:

1o Auditor de código.

2o Biblioteca de soporte de programas.

Auditor de código.

El objetivo principal del auditor de código es controlar la calidad de los programas fuente desarrollados identificando aquellos aspectos que se encuentran fuera de las normas establecidas. El auditor de código no tiene como objetivo optimizar, ni limitar la creatividad del programador; solo se desea, mediante la unificación del estilo obtener programas fuente que presenten una estructura coherente y tengan una mayor claridad.

Biblioteca de Soporte de Programas.

Los programas, si son de buena calidad, una vez escritos son recursos reusables. Es común dedicar tiempo a desarrollar programas que ya existen, dado que su disponibilidad no es conocida por todos. Si existen programas de calidad y son reusables, estos deben agruparse en bibliotecas.

El establecimiento de bibliotecas de módulos reusables no solo reduce el costo y duración de un proyecto al cuidar la duplicación de trabajo dentro de una empresa de desarrollo de programación, sino también favorece al control de calidad, empleando módulos o programas ya probados. En algunos proyectos no es posible emplear módulos reusables, pero aún en estos casos el establecimiento de una biblioteca de soporte de programas es muy efectivo. Aún cuando los módulos hayan sido realizados para satisfacer una necesidad muy específica, su introducción a una biblioteca de soporte de programas permite el control del avance del proyecto, da acceso a la última versión actualizada de los módulos y permite sistematizar el registro de los cambios realizados.

Solamente el empleo de las herramientas automáticas permite establecer y mantener bibliotecas de módulos.

La biblioteca de soporte de programas es una herramienta automática necesaria para apoyar el desarrollo de sistemas. El objetivo principal de la biblioteca es proveer continuamente programas

fuentes actualizados y legibles, tanto por el ser humano como para la computadora. Estos programas para formar parte de la biblioteca deben ser debidamente acreditados por el usuario final y cumplir con las normas de control de calidad establecidas.

Para introducir un programa a la biblioteca es necesario que el usuario llene una forma de transmisión de información que contiene la información necesaria para introducir un programa fuente. La información referente al programa se almacena en la base de datos de la biblioteca de soporte de programas.

Diversas causas pueden dar origen a la necesidad de realizar cambios a los programas de la biblioteca. Durante el desarrollo del sistema pueden aparecer cambios a los requerimientos, mejoras al producto o errores en el código. Cualquiera que sea la causa para realizar un cambio; estos cambios son registrados en la base de datos de la biblioteca.

La biblioteca de soporte de programación siempre mantiene intacta la versión original de un programa fuente y genera la versión actual a partir de una bitácora de cambios. Esto permite tener una historia de los cambios hechos a un programa y así, en un momento dado, poder tener cualquier versión del mismo. El código generado durante todo el proyecto se lleva en listados, junto con la historia de las modificaciones. Varios reportes pueden ser obtenidos de la biblioteca

de soporte de programación, tales como el catálogo de programas fuente en biblioteca.

La función de control de calidad desempeña un papel importante en la administración de un proyecto de programación. El jefe de control de calidad realiza las funciones de un auditor al servicio del jefe del proyecto verificando que las normas sean observadas y que la documentación se mantenga al día. A pesar de su función de supervisión si el control se maneja con diplomacia y las normas son lógicas y bien definidas y fueron desarrolladas buscando en consenso de los integrantes del grupo su función será bien recibida. Control de calidad deberá convencer a los grupos de trabajo de que su función evita problemas y garantiza el éxito del proyecto. También ayuda a esta función de auditoría el empleo de herramientas automáticas, que serán usadas por los programadores durante el desarrollo del proyecto, garantizando que posteriormente sus productos pasen la auditoría de calidad sin dificultad. La auditoría deberá llevarse al cabo durante el desarrollo del proyecto en forma continua y no justamente antes de liberar la documentación, para:

- a) Identificar y documentar las características físicas y funcionales de los elementos que serán administrados.
- b) Controlar los cambios en los productos de programación.
- c) Registrar y reportar los procesos de cambio y su implantación.

Los elementos controlados por la administración de la configuración son los productos y los sistemas de los cuales se desea supervisar contenido y formato.

Administración del Desarrollo de la Programación.

Ninguna actividad de administración podrá considerarse completa si no se tiene un programa para revisar siempre los resultados que se van obteniendo durante el desarrollo del proyecto y para implantar acciones correctivas si estos resultados difieren de los esperados. Por ello es necesario revisar continuamente los resultados y realizar modificaciones y correcciones cuando sean necesarias.

Como todos los proyectos deberán realizarse dentro de un marco de referencia temporal fijar el tiempo disponible para la realización de las diferentes actividades. Además en alguna de éstas será necesario realizar inversiones, es decir, asignar recursos materiales que tienen cierto valor.

Como los beneficios del proyecto, en general, no se empiezan a percibir antes de su terminación, cualquier atraso en la ejecución del mismo implicará demoras en la recuperación de la inversión. Por ello los tiempos de realización de cada actividad del proyecto, que desde luego afectan el tiempo de desarrollo del conjunto, son de gran importancia.

Complejidad de la programación.

Los costos de mantenimiento de un programa pueden llegar a ser del orden del 40 al 70%¹² de los costos totales de programación. Por esta razón, cualquier medida que se tome para disminuirlos tendrá un efecto muy importante sobre el costo de la programación.

Métodos para el Control de Calidad en el Desarrollo de Software.

Autopruebas.

Son todas las actividades que un ingeniero de sistemas puede ir realizando para evaluar la Calidad del producto antes de presentarlo. Estas actividades las podremos considerar como pruebas privadas.

Lista de Pendientes (Checklists).

Es una lista de los errores u omisiones que se cometen frecuentemente y se utiliza como una ayuda a la memoria. Esta lista se utilizará leyendo cada oración y verificando lo que se pregunte sobre lo requerido.

¹²Desarrollo y Administración de Programas de Computadora (sep/85)

Pruebas de Escritorio.

Es una técnica para descubrir errores en el producto de software. Se efectúa leyendo el código del programa para buscar los errores de lógica y de sintaxis, para esto se seguirá la lógica del programa haciendo las veces de la computadora.

Para describir errores de sintaxis se lee línea por línea y se pueden hacer listas de referencias cruzadas.

Pruebas Unitarias.

Son pruebas privadas que se hacen antes de integrar las diferentes partes de un sistema y hacer las pruebas al sistema. El número de errores y defectos encontrados con las pruebas unitarias no se registra, esto no quiere decir que estas pruebas sean tiradas a la basura. La metodología de pruebas debe seguir y mantener una contabilidad de errores personal.

Pruebas Estáticas.

Son las pruebas en las que no se ejecuta nada en la computadora. Es un proceso humano. Durante estas pruebas se compara el producto contra sus requerimientos o especificaciones.

Revisiones.

Es un grupo de exámenes que se realizan durante la vida del sistema. Estas revisiones tienen lugar a través del ciclo de vida del sistema y pueden ser desde revisiones públicas por supervisores o

revisiones muy privadas para ayudar durante el proceso de desarrollo. En una revisión se discuten los objetivos. El grupo que realiza las revisiones debe preguntar, buscar respuestas claras y señalar las posibles áreas de problema.

Auditorías.

En ésta etapa se verifica que las tareas requeridas para una actividad se hayan cumplido. Normalmente en una auditoría se utilizan listas de puntos que son publicadas con anterioridad. Confirman que la documentación esté completa, que las revisiones requeridas, las inspecciones y las pruebas se hayan realizado y que todos los problemas se hayan registrado y corregido.

Uno de los beneficios de realizar auditorías es que los desarrolladores sepan que se les hará una auditoría. Si ellos conocen lo que se les verificará, podrán asegurarse de cumplirlo. Las auditorías no se concentran en problemas técnicos ó explicaciones, sino en lo que actualmente se tiene ya terminado.

Pruebas Dinámicas.

Las pruebas dinámicas confirman que el software cumple los requerimientos y las especificaciones. En contraste con las pruebas estáticas, las pruebas dinámicas se hacen con una ejecución del Software actual por una simulación de un proceso no automatizado. Se compara la funcionalidad del Software con sus requerimiento, y la estructura del programa con los estándares internos.

Planes de Prueba.

Un plan de pruebas describe los acercamientos, las fuentes y el horario de las actividades de las pruebas. Identifica los elementos que deben ser examinados, las características a ser probadas, las tareas que se deben realizar durante las pruebas, el personal responsable para cada tarea y los riesgos asociados con la prueba.

PRUEBAS DE SISTEMA.

Las pruebas de sistema tienen como propósito comparar el sistema o programa contra sus objetivos originales, contra sus requerimientos de alto nivel. Esto tiene dos implicaciones:

1o Las pruebas de sistemas no están limitadas a "sistemas". Si el producto es un programa las pruebas de sistema serán los procesos que intentarán demostrar que los programas no logran sus objetivos.

2o Por definición, las pruebas de sistemas serán imposibles si el líder de proyecto no ha puesto por escrito los objetivos del mismo.

A continuación se describen 16 categorías que serán aplicables a todos los programas o sistemas, pero para evitar pasar por alto alguna, todas las categorías deben ser verificadas al momento de diseñar los casos de pruebas.

1o Pruebas de Facilidades.

El tipo de pruebas que es más obvio, es en el que se determina si cada una de las facilidades o funciones especificadas en los objetivos fueron alcanzadas. El procedimiento es verificar los objetivos, frase por frase, y cuando en alguna parte se especifique "que", determine si el programa satisface el "que". Este tipo de pruebas puede ser realizada sin el uso de la computadora, es suficiente una comparación mental contra la documentación del usuario.

2o Pruebas de Volumen.

Un segundo tipo de pruebas es someter el programa a grandes volúmenes de información. Cada programa debe exponerse al menos a una prueba de volumen.

3o Pruebas de Stress.

Las pruebas de stress involucran el someter al programa a cargas pesadas. Estas pruebas no deben confundirse con las pruebas de volumen: una carga de stress es recibir un alto volumen de información en un lapso de tiempo muy corto.

Un sistema de tiempo compartido que deba soportar hasta 64 terminales, se someterá al extremo de 64 usuarios tratando de darse entrada simultáneamente en el sistema (ésta no es una situación "que nunca ocurrirá", ocurre en la vida real después de que el sistema se ha caído y es levantado por el operador).

Muchas de las pruebas de stress representan condiciones que el programa tendrá en operación, otras pruebas posiblemente representen situaciones " que nunca ocurrirán " pero ésto no implica que estas pruebas no sean útiles , si se detectan errores con estas situaciones imposibles, estas pruebas serán valiosas porque probablemente surja el mismo error en la realidad en situaciones con menos stress.

4o Pruebas de Sencillez de Uso.

Otra categoría importante de casos de prueba de sistema son aquellas que intentan encontrar factores humanos o problemas de uso.

A continuación se presenta una lista que ilustra los tipos de consideraciones que deben ser probadas.

1o ¿Cada una de las interfaces de usuario ha sido dirigida a la inteligencia y educación del usuario final ?

2o ¿ Las salidas del programa son significativas y no ultrajantes ?

3o ¿ Los mensajes de error están enfocados al usuario final, o alguna requiere la ayuda de experto en computación para poder comprenderlo ?

4o ¿Todas las interfaces del usuario muestran una integridad conceptual considerable; hay consistencia y uniformidad en la sintáxis, convenciones, semántica, formato, estilos y abreviaturas ?

5o ¿ El sistema contiene demasiadas opciones, o hay opciones que probablemente no se usarán ?

6o ¿ El sistema envía algún tipo de aceptación inmediata para todas las entradas ?

7o ¿ Es fácil de usar el programa ?

5o Pruebas de Seguridad.

Debido al aumento de interés de la sociedad en la privacidad, muchos programas tienen objetivos específicos de seguridad. Las pruebas de seguridad intentarán idear casos de prueba que

sobrepasen los puntos de seguridad del sistema. Una manera de idear estos casos es estudiar problemas de seguridad conocidos en sistemas similares y formular casos de prueba que intenten generar problemas idénticos en el sistema en cuestión.

6o Pruebas de Eficiencia .

Muchos programas tienen objetivos específicos de desempeño o de eficiencia, estableciendo propiedades como tiempos de respuesta cantidad de información bajo ciertas cargas de trabajo y condiciones de configuración. Otra vez, como el propósito de las pruebas de sistema es demostrar que el programa no logra sus objetivos, los casos de pruebas deben estar orientados a demostrar que el programa no satisface sus objetivos de desempeño y eficiencia.

7o Pruebas de Almacenamiento.

Similarmente, los programas ocasionalmente tienen objetivos de almacenamiento, estableciendo, por ejemplo, las cantidades de almacenamiento primario y secundario requeridas por el programa.

8o Pruebas de Configuración.

Programas tales como sistemas operativos soportan varias configuraciones de hardware. Normalmente es difícil intentar probar el programa con cada una de las posibles configuraciones debido a que son demasiadas. Sin embargo el sistema se probará con cada tipo de hardware.

9o Pruebas de Compatibilidad/Conversión.

Muchos programas que son desarrollados no son del todo nuevos, sino que reemplazarán a programas deficientes tanto del sistema automatizado como del manual. Los programas tienen frecuentemente objetivos específicos concernientes con su compatibilidad y con sus procedimientos de conversión hacia los sistemas existentes.

10o Pruebas de Instalación.

Algunos tipos de sistemas tienen procedimientos complicados de instalación. Las pruebas para los procedimientos de instalación son parte de los procesos de pruebas de sistema.

11o Pruebas de Confiabilidad.

El objetivo de todas las categorías de pruebas de sistema es la mejora de la confiabilidad actual del programa, pero si los objetivos del programa contienen indicaciones específicas sobre confiabilidad deben de llevarse a cabo estas pruebas. Las pruebas de confiabilidad pueden ser difíciles de llevar a cabo.

12o Pruebas de Recuperación.

Programas como los sistemas operativos o manejadores de bases de datos tienen normalmente objetivos de recuperación de información para cuando sucedan errores de información. El objetivo de estas pruebas es demostrar que éstas funciones de recuperación no funcionan correctamente. Por ejemplo; se puede simular fallas de hardware (errores de paridad, errores de dispositivos) ó errores de

información (ruido en las líneas de comunicación, un apuntador inválido en una base de datos) para analizar las reacciones del sistema.

13o Pruebas de Mantenimiento.

El programa debe tener objetivos acerca de sus características de servicio durante el mantenimiento. Tales objetivos deben definir las ayudas para el mantenimiento del sistema, tiempos aproximados de corregir un error, los procedimientos de mantenimiento y la Calidad de la documentación con el sistema.

14o Pruebas de Documentación.

Sabiendo que los objetivos de los programas no contienen las descripciones precisas de las interfaces externas de los programas, necesitaremos tomar la documentación del usuario para formular los casos de prueba. Los casos de prueba serán diseñados analizando los objetivos y serán formulados analizando la documentación del usuario. Esto tiene un efecto útil extra, comparando el programa no solo contra sus objetivos, sino también contra la documentación del usuario y ésta contra los objetivos.

Las pruebas de sistema dependen de la precisión de la documentación del usuario, porque servirá para establecer la mayoría de los casos de prueba. También la documentación del usuario debe ser revisada en cuanto a precisión y calidad.

15o Pruebas de Procedimiento.

Finalmente muchos programas son parte de sistemas que no son completamente automáticos e involucran procedimientos a realizarse por gente. Todos los procedimientos humanos prescritos, tales como procedimientos a seguir por el operador del sistema, administrador de la base de datos o de usuario de terminal deben ser probados durante las pruebas de sistema.

16o Pruebas de Aceptación.

Estas pruebas serán el proceso de comparar el sistema contra sus requerimientos originales y contra las necesidades actuales del usuario. Estas pruebas son llevadas a cabo por el mismo usuario final. La función del usuario será verificar que lo establecido en el contrato o en la definición del sistema es cumplido.

A continuación daremos a conocer un cuestionario con los conceptos más importantes de este tema.

- 1o. ¿Para la elaboración de un programa es necesario cumplir con las 5 características de requerimientos?
- 2o. ¿Es indispensable la elaboración de un modelo conceptual?
- 3o. ¿Para la realización de un sistema se hacen diagramas de flujo?
¿Por qué?
- 4o. ¿Qué otra técnica usa?
- 5o. ¿Cómo pueden hacer la identificación de los programas?

60. ¿Se hacen anotaciones en caso de que se sucedan eventos no esperados al ir realizando el programa?
70. ¿Al finalizar la arquitectura de un sistema se anotan los nombres y responsabilidad de las personas encargadas?
80. ¿Existe un grupo o una persona encargada de la calidad de la programación?
90. ¿Qué puesto ocupa dentro del área?
100. ¿Utilizan normas de requerimientos del programa?
110. ¿Cuáles son las normas de programación que siguen?
120. ¿Se utiliza el auditor de código y/o biblioteca de soporte de programas como herramientas automáticas?
130. ¿Utilizan alguna otra?
140. ¿Se lleva bitácora?
150. ¿Cada cuanto tiempo se lleva?
160. De los siguientes métodos de control de calidad cuáles se utilizan:
- | | | | |
|-------------------------------------|-----|----------------------|-----|
| a) Autopruebas | () | f) Revisiones | () |
| b) Lista de pendientes (checklists) | () | g) Auditorías | () |
| c) Pruebas de escritorio | () | h) Pruebas dinámicas | () |
| d) Pruebas unitarias | () | i) Planes de pruebas | () |
| e) Pruebas estáticas | () | | |

17o. De las siguientes categorías de pruebas de sistemas cuáles se llevan a cabo?

- | | | | |
|---------------------------|-----|-------------------------|-----|
| a) P. de Facilidades | () | j) P. de Compatibilidad | () |
| b) P. de Volumen | () | k) P. de Instalación | () |
| c) P. de Stress | () | l) P. de Confiabilidad | () |
| d) P. de Sencillez de Uso | () | m) P. de Recuperación | () |
| e) P. de Seguridad | () | ñ) P. de Mantenimiento | () |
| g) P. de Eficiencia | () | o) P. de Documentación | () |
| h) P. de Almacenamiento | () | p) P. de Procedimiento | () |
| i) P. de Configuración | () | q) P. de Aceptación | () |

CAPITULO V

EVALUACION DEL PROCESO DE DATOS Y DE LOS EQUIPOS DE COMPUTO.

Los datos son uno de los recursos mas valiosos de las organizaciones y, aunque son intangibles, necesitan ser controlados y auditados con el mismo cuidado que los demás inventarios de la organización, por lo cual se debe tener presente:

1o La responsabilidad de los datos es compartida conjuntamente por alguna función determinada de la organización y de la dirección de informática.

2o Un problema que se debe considerar es que se origina por la duplicidad de los datos y consiste en poder determinar los propietarios o usuarios posibles (principalmente en el caso de redes y bases de datos) y la responsabilidad de su actualización y consistencia.

3o Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas en general.

4o Se deben de relacionar los elementos de los datos con las bases de datos donde están almacenados, así como los reportes y grupos de procesos donde son generados.

La mayoría de los delitos por computadora son cometidos por modificaciones de datos al:

- Suprimir u omitir datos.
- Adicionar datos.
- Alterar datos.
- Duplicar procesos.

Esto es de suma importancia en caso de que equipos de cómputo que cuentan con sistemas en línea, en los que los usuarios son los responsables de la captura y modificación de la información al tener un adecuado control con señalamiento de responsables de los datos (uno de los usuarios debe ser el único responsable de determinado dato), con claves de acceso de acuerdo a los niveles.

- PRIMER NIVEL: puede hacer únicamente consultas.
- SEGUNDO NIVEL: puede hacer captura, modificaciones y consultas.
- TERCER NIVEL: sólo puede todo lo anterior y además realizar bajas.

Los instructivos de operación proporcionan al operador información sobre los procedimientos que debe seguir en situaciones normales y anormales en el procesamiento, y si la documentación es incompleta o inadecuada lo obliga a improvisar o suspender los procesos

mientras investiga lo conducente, generando probablemente errores, reprocesos, desperdicio de tiempo de máquina, se incrementan, pues, los costos del procesamiento de datos.

La función clave del programador de cargas de máquina está relacionada con el logro eficiente y efectivo que:

- Satisfaga las necesidades de tiempo del usuario.
- Sea compatible con los programas de recepción y transcripción de datos
- Permiten niveles efectivos de utilización de los equipos y sistemas de operación.
- Es ágil la utilización de los equipos en línea.

Se deberán evaluar los procedimientos de programación de cargas máquina para determinar si se ha considerado atenuar los picos de los procesos, generados por cierres mensuales, y poder balancear las cargas de trabajo de línea, dando prioridad a los procesos en línea.

Se deberá procurar que la distribución física del equipo sea funcional, que la programación de las cargas de máquina satisfaga en forma eficaz al usuario; se tendrá cuidado con los controles que se tengan para la utilización de equipo y que el mantenimiento satisfaga las necesidades del equipo.

Los dispositivos de almacenamiento representan , para cualquier centro de cómputo, archivos extremadamente importantes cuya

pérdida parcial o total podría tener repercusiones muy serias, no sólo en la unidad de informática, sino en la dependencia de la cual se presta servicio. Una dirección de informática bien administrada debe tener perfectamente protegidos estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza (borrado de información), principalmente en el caso de cintas.

Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando además los tiempos de proceso.

Para evaluar el mantenimiento del equipo, no se debe olvidar que la capacidad bruta disponible se deberá disminuir por las actividades de mantenimiento preventivo, fallas internas y externas no previstas y mantenimiento e instalación de nuevos sistemas.

TIPOS DE MANTENIMIENTO

Existen 3 tipos de contratos de mantenimiento:

a) Total que incluye el mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no incluye partes.

b) Es "por llamada", en el cual en caso de descompostura se le llama al proveedor y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para componerlo. Este tipo de mantenimiento no incluye refacciones.

c) Este se conoce como "en banco", y aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y éste hace una cotización de acuerdo con el tiempo necesario para su compostura más las refacciones.

Los dispositivos del sistema de cómputo, los archivos magnéticos, pueden ser dañadas si se manejan en forma inadecuada y eso puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Se debe de revisar las disposiciones y reglamentos que contribuyan al mantenimiento del orden dentro de la sala de máquinas.

En la productividad el objetivo es evaluar la eficiencia con que opera el área de captación y producción.

1o Verifique que se cuente con una descripción completa de los trabajos que se corren y la descripción de las características de carga.

2o Verificar la existencia de un pronóstico de cargas o trabajos que se efectuarán durante el año, con el objeto de que se prevean los picos en las cargas de trabajo y se puedan distribuir adecuadamente estas cargas.

3o Verificar que se contemplen dentro de los planes de producción periodos de mantenimiento preventivo.

4o Verificar que se disponga de espacio y tiempo para realizar corridas especiales, corridas de prueba de sistemas en desarrollo y corridas que deben repetirse.

5o Verificar que se tengan definidos el espacio y tiempo para el respaldo de la información.

Los auditores deben de adquirir un conocimiento general del sistema informático al mismo nivel que conocen los sistemas contables de las empresas. Deben conocer los puntos fuertes y débiles del funcionamiento del sistema informático y aquellos en los que pueda darse el caso de que los procedimientos fallen.

Los auditores informáticos deberán tener también una visión muy clara de cuál es su papel respecto de la jefatura de proceso de datos, y

cada una de ellos deberá comprender la posición del otro. El auditor puede proporcionar al jefe de proceso de datos un análisis independientemente de procedimientos y sistemas, lo que debería suponer una seguridad suficiente.

La jefatura de proceso de datos y la de la empresa tienen la responsabilidad de diseñar, implantar y explotar unos sistemas informáticos precisos, fiables y seguros. Una vez asumido el trabajo de auditoría, será necesario que el auditor informático se relacione estrechamente con el personal de proceso de datos, porque a menudo necesitará hacer un seguimiento rápido de su trabajo. Sin embargo se deben tomar precauciones para asegurar que el auditor no asuma responsabilidades de jefatura, viéndose involucrado en las etapas de diseño o perder las posibilidades de hacer un análisis independiente y crítico.

En relación con los temas técnicos, los auditores pueden necesitar obtener ayuda del equipo del departamento informático o también, información sobre equipos, sobre cómo ejecutar paquetes, sobre temas de programación, sobre procedimientos y explotación del ordenador y sobre la interpretación de la documentación. Los auditores podrán seguir estos consejos siempre que adopten las precauciones normales y hagan las comprobaciones oportunas.

A continuación daremos a conocer un cuestionario para basarnos en lo más importante de este capítulo.

- 1o. ¿Existen claves de acceso para los usuarios de acuerdo al nivel que jerárquico?
- 2o. ¿Cuántos y cuáles son los niveles existentes?
- 3o. ¿Existen instructivos de operación?
- 4o. ¿Existen dispositivos de almacenamiento?
- 5o. ¿Se tiene algún contrato de mantenimiento?
- 6o. ¿Qué tipo de mantenimiento es y cuál es su cobertura?
- 7o. ¿Cada cuánto se le da mantenimiento al equipo?

CAPITULO VI

EVALUACION DE LA SEGURIDAD.

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

Al auditar los sistemas, se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

El crecimiento de los fraudes por computadora ha hecho patente que la potencialidad de las faltas crece en forma más rápida que en los sistemas de seguridad.

Los motivos de las faltas por computadora normalmente son por:

- Beneficio personal.
- Beneficios para la organización.
- Por beneficiar a otras personas (Síndrome de Robin Hood).
- Fácil desfalcar.
- El departamento es deshonesto.

- El individuo tiene problemas financieros.
- Equivocación de ego (deseo de sobresalir en alguna forma).
- Mentalidad turbada.

El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos al de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

En la actualidad las compañías cuentan con grandes dispositivos de seguridad física de las computadoras y se tiene la idea que los sistemas no pueden ser violados si no se entra al centro de cómputo, olvidándose del uso de terminales y de sistemas remotos de teleproceso.

Los sistemas de seguridad normalmente no consideran la posibilidad de fraude cometida por los empleados en el desarrollo de sus funciones. La introducción de información confidencial a la computadora puede provocar que este concentrada en las manos de unas cuantas personas y una alta dependencia en caso de pérdida de los registros. El más común de estos delitos está dado en el momento de programación, en el cual por medio de ciertos algoritmos se manda borrar un archivo.

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

El sistema integral de seguridad debe comprender:

- Elementos administrativos.
- Definición de una política de seguridad.
- Organización y división de responsabilidades.
- Seguridad física y contra catástrofes.
- Prácticas de seguridad del personal.
- Pólizas de seguros.
- Sistemas de seguridad de equipos y de sistemas, incluyendo todos los elementos, tanto de redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos.
- El papel de los auditores, tanto internos como externos.
- Planeación de programas de desastre y su prueba.
- Sistema de respaldos.

Uno de los puntos que se debe auditar con más detalle es el de tener las cifras de control y el medio adecuado que nos permita conocer en el momento que se produce un cambio o un fraude en el sistema.

Algunas instalaciones y sus aplicaciones tienen un alto grado de riesgo, con un gran impacto en la organización o en la comunidad, si es que el servicio se interrumpe cierto periodo; otras pueden fácilmente continuar sin afectar grandemente a la organización por medio de utilización de métodos manuales.

En el caso de sistemas como el de reservaciones, bancos o casas de bolsa, el único procedimiento para evitarlos es tener sistemas simultáneos (tándem o en paralelo) que permitan pasar de un equipo a otro en forma instantánea, disponer de sistemas duplicados en áreas críticas (aires acondicionados, discos, etc.) y tener sistemas de energía no interrumpible (no break), ya que debido a su alto riesgo son los que deben tener mayor seguridad.

En la actualidad los programas y los equipos son altamente sofisticados y sólo algunas personas dentro del centro de cómputo conocen al detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no toman las siguientes medidas:

- 1o Se debe restringir el acceso a los programas y a los archivos.

- 2o Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.

3o Se debe asegurar en todo momento que los datos y archivos dados sean los adecuados, procurando no usar respaldos inadecuados.

4o No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.

5o En los casos de información confidencial debe usarse, en forma codificada.

6o Se debe realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.

7o Se debe monitorear periódicamente el uso que se les está dando a las terminales.

8o Se deben hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.

9o Debe controlarse la distribución de las salidas.

10o Se deben guardar respaldos de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad. (bancos).

11o Se deben identificar y controlar perfectamente los archivos.

12o En el caso de programas, se debe asignar a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión.

Esto nos servirá para identificar el número de veces que se ha compilado o corrido un programa, y nos permitirá costear en el momento que se encuentre un sistema en producción.

Cuando realice análisis de seguridad informática y de planificación de emergencia, el auditor:

1o Examinará sistemáticamente todos los riesgos que intervengan y aclararán las pérdidas probables en cada caso.

2o Considerará las maneras de aumentar la seguridad para reducir los riesgos.

3o Recomendará todas las acciones necesarias de protección encaminadas a reducir el riesgo de que se produzca una interrupción importante de la capacidad de proceso de datos de la empresa, o sugerirá los planes de emergencia para afrontar dicha interrupción, en caso de que se produzca.

4o Cuando corresponda, estudiará la cobertura de seguros de la empresa.

Riesgos.

Los riesgos siguientes son los más frecuentes que pueden afectar a la continuidad de las operaciones del departamento de proceso de datos de la empresa.

Incendios: Por la cantidad de equipo eléctrico complicado que hay en las salas de equipos, existe un riesgo de incendio superior a la media. La mayoría de los incendios son pequeños, pero alrededor de una vez al año se produce un importante incendio en algún lugar, que destruye completamente las instalaciones informáticas.

Inundación: Se han dado varios casos de inundaciones en centros de cómputo, debidas a desbordamientos de niveles de agua, rotura de tuberías, o caída de aguas destinadas a sofocar otros incendios. El agua puede perjudicar permanentemente el equipo.

Avería de los equipos auxiliares: Los ordenadores han quedado inutilizados por fallos del sistema de aire acondicionado, del suministro eléctrico, etc.

Acciones malintencionadas: Se han dado casos en que los operadores u otras personas han agredido físicamente a los ordenadores o han destruido intencionalmente ficheros importantes.

Robo de información: Están aumentando los casos de venta de información reservada, como listas de clientes o de personal, en cinta magnética o en disco.

Relaciones laborales: Muchos sindicatos se han dado cuenta de que las huelgas selectivas o incluso las huelgas de celo realizadas en los centros de cómputo, pueden inutilizar pronto a una empresa. El transcurso de una auditoría, el auditor estimará que puede existir la necesidad de limitar los daños que pudieran causarse, o que la moral del personal fuese anormalmente baja, lo reflejará en su informe a la dirección.

Pérdidas y fraude.

Las pérdidas pueden darse por diversos motivos, por ejemplo, a causa de errores. En los sistemas grandes y complejos, que tienen muchos programas, es muy probable que se produzcan errores. A pesar del cuidado y del control que se pongan, es posible que queden errores sin telear, que pueden dar lugar a pérdidas. Las pérdidas se deben a veces a mala gestión y a la falta de control. También pueden tener su origen en acciones deliberadas y fraudulentas. En ciertos casos la naturaleza de las pérdidas pueden tener su origen en fraudes, en vez de errores. El fallo de una persona o de una sección puede ser descubierto o explotado fraudulentamente por un tercer. Podría ser difícil distinguir entre pérdida y fraude, porque la diferencia podría residir totalmente en el motivo.

Los sistemas mecanizados son susceptibles de pérdidas o fraudes debido a que:

a) Tratan grandes volúmenes de datos e interviene poco personal, lo que impide verificar todas las partidas.

b) A veces se graban los registros magnéticos, perdiéndose la evidencia auditable o la secuencia de acontecimientos.

c) A veces, los registros magnéticos son transitorios y a menos que se realicen pruebas dentro de un periodo de tiempo corto, podrían perderse los detalles de lo que sucedió, quedando sólo los efectos.

d) Los sistemas son impersonales, aparecen en un formato ilegible y están controlados parcialmente por personas cuya principal preocupación son los aspectos técnicos del equipo y del sistema y no comprenden, o no les afecta, el significado de los datos que manipulan.

e) En el diseño de un sistema importante es difícil asegurar que se han previsto todas las situaciones posibles y es probable que en las previsiones que hayan hecho queden huecos sin cubrir. Los sistemas tienden a ser algo rígidos y no siempre se diseñan o modifican al ritmo con que se producen los acontecimientos.

f) Sólo parte del personal de proceso de datos conoce todas las implicaciones del sistema y del centro de cómputo puede llegar a ser un centro de información. Al mismo tiempo, el centro de cómputo procesará muchos aspectos similares de las transacciones.

g) En el centro de cómputo hay un personal inteligente, que trabaja por iniciativa propia la mayoría del tiempo y podría resultar difícil implantar unos niveles normales de control y supervisión.

h) Cuando surgen discrepancias, no se imagina que se han producido un fraude, y la investigación puede abandonarse antes de llegar a esa conclusión. Se tiende a empezar buscando errores de programación y del sistema. Si falla ésta operación, se buscan fallos técnicos y operativos. Sólo cuando todas estas averiguaciones han dado

resultado negativo, acaba pensándose en ciertas circunstancias en que la causa podría ser un fraude.

Fraude Informático.

El fraude informático es uno de los dos tipos básicos de fraude al que están expuestos los sistemas mecanizados. Estos fraudes suelen ser derivaciones simples de los que se realizan en los sistemas manuales e implican normalmente la introducción de transacciones fraudulentas; por ejemplo:

- a) Notas de gastos incorrectas.

- b) Recibos de salarios incorrectos.

- c) Notas de abono a clientes con los que el defraudador está en conveniencia.

- d) Descuentos favorables a clientes que estén en conveniencia con el defraudador.

- e) Creación de cuentas ficticias a beneficio del defraudador, por ejemplo, crear registros falsos de empleado en la nómina para que el defraudador reciba más salario.

f) Pasar dos veces las mismas transacciones utilizando los sistemas normal y "urgente" o de "respaldo" y explotar la debilidad de los controles.

En otros casos, el fraude podría radicar en la modificación de transacción verdaderas en beneficio del defraudador o de algún cómplice. Por ejemplo, el empleado deshonesto puede modificar el código de transacción de modo que los envíos que se hagan a un cliente que esté en complicidad con dicho empleado, se traten como muestras o como reposición por rotura.

Función de los auditores internos y externos.

Con la frecuencia, se experimenta sorpresa al descubrir que la función de auditoría es una parte del concepto de seguridad total. Hasta ahora se ha tratado de demostrar que cada elemento del concepto es importante, tanto de manera aislada como al formar parte integral del mismo. El objetivo es demostrar que la función de auditoría es un elemento muy importante.

En consecuencia, aunque se resumen el alcance y las funciones de los auditores tanto internos como externos y se destacan cuidadosamente los aspectos sobresalientes de la auditoría computacional y el impacto que tienen sobre la seguridad en computación no se presenta una exposición en detalle de las técnicas de auditoría computacional.

Audidores externos.

El auditor externo puede asumir un trabajo especial. Esto sin embargo, casi nunca impide al auditor realizar su función primaria de expresar una opinión acerca de la contabilidad producida por una institución con base en el examen de los libros e informes. Es decir, contrariamente a la creencia general, el auditor no es responsable de la detección de fraudes.

Audidores internos.

El alcance de sus actividades varía de una institución a otra. Algunas veces, desempeña de alto nivel que consisten en informar sobre la efectividad gerencial de la institución, en otras, su función principal es verificar los sistemas y procedimientos y encargarse de que se refuercen.

De este modo, el papel del auditor interno, que ha involucrado durante los últimos 50 a 75 años, no es una extensión de la función del auditor externo. Por el contrario el auditor interno es, en gran medida, una parte de los sistemas de control interno dentro de una institución. Esta es la manera como ha evolucionado la función del auditor interno: una forma de inspector interno.

Con frecuencia, el rol del auditor interno es más bien reducido que amplio. No obstante la tendencia actual indica una ampliación de funciones, ya que el auditor interno realiza auditorías de gerencia y operativas. Dentro de este contexto, el auditor interno también se

familiariza más con la computación. Muchos de los grandes usuarios de computadoras, donde se han dado aplicaciones de mayor complejidad, han reconocido la necesidad de una mayor participación de la función de auditoría interna. Así, las actividades del auditor interno abarcan, por lo general:

1o Participación, activa en el proceso de desarrollo, al garantizar la incorporación de las medidas adecuadas de seguridad y auditoría y también al colaborar con las revisiones de los puntos de verificación del proceso.

2o Revisión de sistemas y controles de la aplicación tanto en los departamentos de usuarios como en los centros de procesamiento computacional.

3o Revisión de la política y los procedimientos de seguridad en computación, y participación activa en las pruebas contra desastres.

4o Introducción de técnicas avanzadas para la auditoría de los sistemas computacionales complejos.

De acuerdo con lo anterior, la relación informativa del auditor interno se ha elevado y, en muchos casos, él ahora informa a un miembro de la mesa directiva o algún otro ejecutivo.

De este modo, se ve cómo el auditor interno maneja un alcance muy amplio de responsabilidades diferente al del auditor externo. El único impacto real que tiene uno sobre el otro, es que la actividad que realiza el auditor interno puede liberar al auditor externo de mucho trabajo detallado, debido al perfeccionamiento del sistema del control interno dentro de la organización.

Los auditores externos e internos deben definir muy claramente las exigencias desde el punto de vista de la auditoría, así como los roles y enfoques que adoptarán para satisfacerlas. La aplicación de los principios debe llevar la elaboración de una serie de cuestionarios para la revisión del control interno y para verificar que los sistemas y los procedimientos funcionen de manera adecuada. Se deben compilar los lineamientos para la aplicación de las técnicas mencionadas de auditoría especializada de incluir la programación de auditoría generalizada para comparar y estratificar los archivos, así como extraer muestras estadísticas e informe. La mayor efectividad que resulte debe aumentar la seguridad en computación.

Funciones y seguridad de la Auditoría en Informática.

Los auditores externos como los internos constituyen una forma independiente e importante de verificación de la eficiencia y, por lo tanto, la seguridad de las actividades computacionales. Por lo general, los controles internos y la seguridad son más efectivos en las empresas bien organizadas. Por eso, la existencia de una verificación y de un informe posterior sobre la eficacia de la actividad de cómputo resulta

valiosa. La seguridad se puede mejorar mediante la consideración de los procedimientos vigentes para la prevención de las fallas en seguridad, su detección y los procedimientos de recuperación en caso de desastre.

Para lograr una contribución efectiva de la función de auditoría a la seguridad computacional, se debe considerar cierto número de aspectos importantes:

- a) El alcance de la auditoría interna en la seguridad computacional.
- b) Una relación clara entre auditores internos y externos.
- c) El papel de la auditoría interna en la sociedad.
- d) El papel de la auditoría interna en los sistemas en operación.
- e) La instrucción y capacitación para la auditoría interna efectiva.

Alcance de la auditoría interna respecto a la seguridad en informática.

En el caso de las computadoras, muy pocos auditores tienen los conocimientos técnicos profundos que les permitan participar activamente dentro del sistema de cómputo y no alrededor de él. Con mucha frecuencia, existe un vacío en la comunicación, es decir, que los

auditores rara vez cuentan con alguna experiencia sobre computación y muy pocos empleados de cómputo han tenido experiencia extensa en auditorías. Muchas veces ésta situación conduce a la oposición activa de los auditores para realizar auditorías completas sobre las actividades complejas de los sistemas de cómputo, programación u operación. Esto disminuye de manera sustancial la contribución que la actividad de la auditoría interna puede ofrecer a la seguridad en computación.

El auditor interno tiene una función importante de participar tanto en la planeación de aplicaciones a largo plazo como en el diseño y la realización de aplicaciones en detalle; de este modo, garantiza que se consideren desde el comienzo las necesidades de seguridad y de auditoría. Al mismo tiempo, el auditor interno puede ofrecer un enfoque independiente para los proyectos de mayor magnitud. Debido al incremento en el número de sistemas avanzados y de gran escala, estas contribuciones aumentan la confiabilidad del progreso en el desarrollo del sistema y evitan los consecuentes gastos innecesarios.

Función en los sistemas en operación.

El auditor interno desempeña un papel importante como mediador entre los controles usuario y los del centro de cómputo; provisto del entrenamiento adecuado, puede conducir las revisiones detalladas de los controles en el usuario y realizar el seguimiento a través de los datos hasta el mismo procesamiento de cómputo. Esta función es muy importante para prevenir abusos en las aplicaciones operativas.

Ningún sistema es estático y las exigencias organizacionales cambia en forma continua. Así los sistemas en operación están sujetos a modificaciones repetitivas y sobre la marcha. Por ello es importante que se efectúe de manera rutinaria una evaluación independiente sobre el espectro completo de la aplicación. Esto constituye sin duda, una área de gran responsabilidad del auditor interno, por lo que los objetivos y el enfoque que se adopten para afrontarla de deben estructurar cuidadosamente.

La organización y los procedimientos inherentes a la función de cómputo tienen gran impacto sobre la efectividad y seguridad de las aplicaciones computacionales. Por lo tanto es importante que el auditor interno reciba la capacitación apropiada para revisar ésta área.

Instrucción y capacitación.

Gran parte de la capacitación se centra en aspectos técnicos y se le da muy poca atención a sus funciones independientes de la máquina. La necesidad más importante de capacitación reside en la aplicación de métodos administrativos probados para el área nueva de cómputo en general y la seguridad computacional en particular.

Lo anterior también sucede con la función de auditoría. Las prácticas y procedimientos de auditoría existen desde hace mucho tiempo. Lo que se necesita es la comprensión de los aspectos técnicos para que los principios establecidos se puedan aplicar de manera apropiada. Algunas de las áreas nuevas como los sistemas de bases de datos, en

en línea y de tiempo real, así crean nuevas diferencias. Sin embargo los principios no cambian, es la aplicación lo que varía.

Uno de los problemas más grandes para garantizar que la función de auditoría contribuya en forma realista con la seguridad computacional, es conseguir el personal adecuadamente capacitado. Durante procedimientos de auditoría. Se agrega a esto la necesidad de contar con habilidades de cómputo y el puesto, resulta más complicado. Otro factor adicional es que ha habido muy poca capacitación disponible para auditores o gerentes acerca de los objetivos, el alcance y el enfoque de la auditoría en informática, el enfoque de la gerencia sobre la seguridad computacional.

Para lograr una contribución efectiva con la seguridad, existen ciertas áreas diferentes que se deben cubrir por la capacitación de auditores y gerentes:

1o Los objetivos de los controles de la aplicación, las medidas de seguridad y los procedimientos de recuperación.

2o La responsabilidad del control interno.

3o La función y el alcance de la auditoría interna.

4o Las necesidades de control especializado en aplicaciones avanzadas; la capacitación de analistas de sistemas, diseñadores y auditores.

5o Métodos de auditoría avanzados para los auditores.

Sólo algunas de éstas áreas se pueden cubrir con los proveedores de computadoras o los institutos de administración.

A continuación se dará un cuestionario como base de los principales conceptos para la práctica.

- 1o. ¿Existen sistemas paralelos?
- 2o. ¿Se hacen respaldos de los archivos y programas?
- 3o. ¿Cada cuánto tiempo?
- 4o. ¿Se guardan en algún lugar seguro?
- 5o. ¿Quiénes tienen acceso?
- 6o. ¿Se lleva bitácora?
- 7o. ¿Existen extinguidores contra incendios?
- 8o. ¿Se saben usar?
- 9o. ¿Cuántos existen?
- 10o. ¿A existido alguna inundación o incendio? ¿Cuál fue la causa?
- 11o. ¿Se han dado casos en que los operadores u otras personas han agredido físicamente a los ordenadores o han destruido intencionalmente ficheros importantes?
- 12o. ¿A existido algún robo de información?
- 13o. ¿Qué tipo de información?
- 14o. ¿Qué cargo tenía?

CONCLUSIONES.

En la actualidad el profesionalista debe de actualizarse en el uso adecuado de las computadoras y en la evaluación que se haga de este recurso tan costoso e indispensable.

También debe adecuarse a las normas de auditoría y del control interno para que sean congruentes con el desarrollo tecnológico. La auditoría en informática es una nueva materia que es consecuencia directa del desarrollo en el área y de la necesidad de evaluar la adecuada utilización, respaldo y confidencialidad de la información de la organización.

Esta nueva área evalúa la información desde su generación (dato) hasta su utilización (información), y debe considerar la herramienta que se utiliza, su optimización, el respaldo de la información y seguridad de la misma, y conseguir el mejor uso de la información al menor costo, evitando duplicidad.

La auditoría no debe terminar con la presentación sino, ser el inicio de una serie de auditorías y revisiones periódicas con un adecuado seguimiento de las observaciones para lograr las correcciones a los problemas y las mejoras a los sistemas que lo ameriten.

Se demostró con el presente trabajo que el concepto de pruebas se extiende más allá de una etapa de pruebas que se realiza al final del proyecto.

El hecho de involucrar más al usuario en el desarrollo de sus sistemas, ayuda a que sus expectativas y necesidades sean cubiertas. Después de todo la gente de Sistemas no lo sabe todo y el único experto en áreas y ramas específicas es el mismo usuario.

La solución más viable ante los inconvenientes presentados es que la Dirección y la Gerencia estén convencidos de la importancia de contar con metodologías de pruebas apropiadas implantadas en todos sus departamentos de desarrollo para que exijan y apoyen la Implantación

de alguna. De hecho la Dirección y Gerencia deben estar preocupadas por tener y aplicar una Auditoría en Informática, como lo están por cumplir los requerimientos de la más estricta Auditoría, inclusive el control sobre el uso de pruebas debe de estar incluida en cualquier auditoría de sistemas.

Las funciones de auditoría tanto interna como externa cumplen un papel importante en la seguridad en computación.

Durante mucho tiempo se ha reconocido la necesidad de contar con la participación extensa de la auditoría interna en los sistemas y seguridad computacionales. En la práctica, muy pocas instituciones han logrado éxito. Probablemente el obstáculo mayor en este sentido es el logro de un compromiso real de la Gerencia, el personal de cómputo y los auditores para aplicar los procedimientos. El confirmar de la capacitación efectiva facilitará esto en gran medida.

Con lo desarrollado se quiere dar un panorama en cuanto a la teoría, pues existen muchas cosas con respecto a la práctica y esto es sólo el

asentamiento de las bases para dar el primer paso en lo que se refiere a la Auditoría en Informática lo anterior aunado con el Boletín 5080 del libro de Normas y Procedimientos de Auditoría se complementaría la teoría con la práctica ya que dicho boletín es el fin de una auditoría.

GLOSARIO

Almacenamiento de datos: El almacenamiento de transacciones o registros a fin de que puedan extraerse cuando se solicite.

Archivo: Grupo de registros tratados como una unidad. La mayor unidad de datos y recuperación del sistema operativo, consistiendo de una colección de datos en uno de varios arreglos descritos por el control de información al cual el sistema tiene acceso.

Arquitectura: Diseño y estructura de el software y/o hardware, de los componentes que consta el sistema.

Auditoría periódica: La verificación de un archivo o de una fase de procesamiento, que tiene por objeto detectar problemas y estimular el cumplimiento futuro con procedimientos de control.

Base de datos: Conjunto de datos que afectan a una serie de aplicaciones o programas que se construyen para facilitar la actualización de datos una sola vez y el acceso y recuperación de información independiente.

Biblioteca: Un lugar especial donde se almacenan cintas magnéticas y discos que se utilizan en el procesamiento en computador con el fin de proporcionar un elemento de control acerca de los mismos de forma que pueda disponerse fácilmente de ellos cuando se requiera y queden protegidos contra extravíos o destrucción.

Bit: El bloque de información más pequeña que puede manejar una computadora. Un bit es uno (on: activado) o un cero (off: desactivado).

Buffer: (área de almacenamiento temporal) Área de memoria que guarda datos hasta que éstos puedan utilizarse. Cuando se escribe en un archivo de disco.

Byte: Un byte puede almacenar un carácter.

Captura de datos: Obtención de datos mediante un dispositivo que se pueda comunicar con un sistema de cómputo.

Carácter alfanumérico : Algún carácter comprendido entre la A y la Z (mayúscula o minúscula) o entre el cero y el nueve.

CD-ROM: Disco compacto, solo de lectura en memoria; medio de almacenamiento de alta capacidad.

Chip: Pequeña parte de silicon, que transporta el equivalente de un número largo de componentes eléctricos, integrando un circuito.

Codificación: Instrucciones sucesivas que dirigen al computador a efectuar un proceso en particular. El registro de valores o caracteres que tienen significados que no son fácilmente obvios.

Compilador: Un programa de computador que compila instrucciones en lenguaje objeto a partir de oraciones de lenguaje fuente.

Consulta: Una solicitud para obtener información sin alterarla.

Contraseña (password): La autorización para permitir el acceso a información o procesos, por medio de una señal o clave conocida únicamente por los individuos autorizados.

Control de dispositivo: Programa que controla un dispositivo, como una terminal, una unidad de disco, o una impresora.

Control interno: Sistema completo de pruebas y control, tanto manuales como mecanizados, diseñados para garantizar la integridad del sistema informático y los datos que procesa.

Copia impresa: Copia en papel generada por la computadora.

C.P.U.: Abreviatura de unidad central de Procesamiento, ésta parte de la computadora realiza los cálculos y manipula información.

Correo electrónico: Los usuarios de una red pueden intercambiar memorándums y otros tipos de documentos con gran rapidez por medio del correo electrónico.

Corrida: Una ejecución en computador de un programa o de distintas rutinas eslabonadas en tal forma que constituyen en sí mismas una operación completa durante la cual no se requiere intervención manual de parte del operador del computador.

Cursor: Pequeño rectángulo o línea luminosa que sale en la pantalla de la computadora e indica donde aparecerá el próximo carácter.

Datos: En la terminología de computación, los hechos, la información o los caracteres que procesa, almacena o produce una computadora.

Densidad: Es la medida de cuanta información puede almacenar un disco en un área determinada. Al mejorar la tecnología en discos, estos han logrado desarrollarse en doble y cuádruple densidad, y ahora permiten almacenar el doble y cuádruple de información en el mismo espacio que un disquette de la P.C. original.

Diagrama de flujo: Un diagrama que presenta mediante símbolos y líneas conectoras, ya sea la estructura lógica de un programa de computador o la secuencia de los procesos de un sistema.

Directorio: Es una lista de archivos relacionados. Los directorios ayudan a organizar los discos al agrupar archivos con información similar, así como usted pondría carpetas con información similar en el mismo archivero.

Disco flexible (floppy disc): Medio de almacenamiento de información en discos pequeños removibles (diskettes) de capacidad menor que los discos magnéticos convencionales, pero con beneficios en cuanto a facilidades de manejo/almacenaje y costo.

Diskette: Disco magnético, delgado y flexible que está protegido por una cubierta semirígida en la cual el disco está permanentemente cerrado (3.5 y 5 1/4).

Dispositivo: Aparato mecánico, eléctrico o electrónico con un propósito específico.

Edición (edit): Un término general de control que incluye la verificación de integridad, los dígitos de verificación, las pruebas de razonabilidad, la verificación de límite, la verificación de validez, etc. Generalmente implica la implantación por medio de un programa de computador.

Eficacia: Virtud, actividad, fuerza, para poder obrar.

Eficiencia: Virtud y facultad para lograr un efecto determinado.

Emulador: Un dispositivo del equipo de computación que permite al computador ejecutar programas en lenguaje objeto escritos para un diferente diseño de computador.

Equipo periférico: Las unidades de almacenamiento auxiliar de un computador, utilizadas para la entrada y salida de información. Todos los componentes de un computador distintos a la unidad central de procesamiento y a la memoria principal.

Estándares: Características similares para todos los productos.

File System: Jerarquía de directorios y archivos, este es creado en una partición en el disco y consiste de un número de grupos de cilindros, cada uno de los cuales tiene inodos y bloques de datos.

Hardware: Equipo físico usado en el procesamiento de datos.

Hoja de calculo: Programa para computadora que automatiza los cálculos de una hoja tabular y que le permite controlar presupuestos u otro tipo de operaciones, así como realizar pronósticos de ¿Qué pasaría sí...?

Home: Una parte del file system donde se guarda la información individual de un usuario.

Icono: Representación gráfica de una aplicación o ventana.

Inodo: Parte de un archivo que contiene información sobre este en el file system. Esta información incluye el tipo de archivo, modos de

acceso, número identificador del usuario y grupo, número de bytes en el archivo.

Interfase: Punto de interacción entre dos sistemas o procesos.

Microprocesador: Es el cerebro electrónico de la computadora y supervisa cualquier operación que esta lleve a cabo.

Módem: Dispositivo que modula y demodula la transmisión de datos puede conectarse a una terminal, impresora, servidor, mediante una línea telefónica.

Multitarea: La capacidad de correr (ejecutar) dos o mas programas al mismo tiempo.

Multiusuario: Permite que más de un usuario use el sistema al mismo tiempo.

Programa: Una secuencia completa de instrucciones de máquina y rutinas, que son necesarias para resolver un problema en un computador. Planear el método o procedimiento para resolver un problema, incluyendo la elaboración de las gráficas de flujo y la escritura de las instrucciones que se conoce como codificación.

Programa de base de datos: Es un programa para computadoras que le ayuda a almacenar, ordenar imprimir y recuperar información.

Puerto: Conector en la parte trasera del sistema que sirve para recibir el cable de una impresora, monitor o cualquier otro dispositivo de hardware.

Recuperar: Acción de obtener información específica desde datos almacenados.

Redes: En comunicación de datos es una configuración en la cual dos o más terminales instaladas son conectadas.

Registro: Colección de datos o palabras relacionados tratados como unidad. Por ejemplo en control de inventarios cada factura podría constituir un registro.

Requerimiento: Ejecutar una tarea.

Respaldo (Back-up): Copiar un archivo o un grupo de datos para guardarla como referencia en caso de que el archivo original o grupo de datos sea destruido o averiado.

Seguridad del sistema: Prevención del acceso o el uso de datos o programas sin autorización.

Sintaxis: Es la forma de escribirse una instrucción.

Sistema: El procesamiento de datos es una colección de hombres, máquinas y métodos organizados para cumplir con un grupo de funciones específicas.

Sistema operativo: Software que controla la ejecución de programas de computadora y que provee la planeación, revisión, control de entradas y salidas, conteo, compilación, asignación de almacenamiento, manejo de datos y servicios relacionados.

Software: Programas de computadora, procedimientos, reglas y posiblemente documentación asociada concerniente a la operación de un sistema de procesamiento de datos.

Tarjeta: Es como se conoce usualmente a la tarjeta interfaz. Es una pieza de hardware que se coloca en el interior de la unidad de sistema y que contiene un puerto para conectar algún dispositivo a la computadora.

Teleproceso: Comunicación a distancia como un telégrafo. Transmisión de datos entre un sistema de computación y dispositivos localizados remotamente, los cuales ejecutan la conversión de formato necesario y controlan el rango de comunicación vía satélite.

Terminal: Punto en un sistema o en una red de comunicaciones en la cual los datos pueden ser registrados o borrados.

Usuario: Cualquier persona que requiera el servicio de un sistema de computación.

Virus: Programa desarrollado específicamente para interrumpir su trabajo al dañar archivos, presentar letreros o imágenes, o dejar inoperante la computadora.

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

- Auditoría en Informática.
José Antonio Echenique.
McGraw Hill.
- Administración de Empresas (Teoría y práctica).
Agustín Reyes Ponce.
Limusa
- Normas y Procedimientos de Auditoría.
Instituto Mexicano de Contadores Públicos.
- Desarrollo y Administración de Programas de Computadora.
Victor Gere, Mauricio Mier, Rolando Nieva.
C.E.C.S.A.
- Auditoría Informática.
A.J. Thomas.
Paraninfo
- Análisis y Diseño de Sistemas.
Kendall y Kendall.
Prentice- Hall Hispanoamericana, S.A.
- Seguridad en Centros de Cómputo.
Leonard H. Fine.
Trillas
- Metodología de Pruebas.
Universidad La Salle.
TESIS
- Planeación Estratégica
George A. Steiner.
C.E.C.S.A.

- Auditoría Administrativa.
William P. Leonard.
Diana.

- Elementos de Auditoria
Mendivil Escalante
E.C.A.S.A.

- La Auditoría Operacional del Depto de Crédito y Cobranzas
E.S.C.A.
TESIS

- Fundamentos de Administración
Munch Galindo/ García Martínez
Trillas