UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES "ACATLAN"

AUDITORIA INFORMATICA

TESIS QUE PARA OBTENER EL TITULO DE LICENCIADO EN MATEMATICAS APLICADAS Y COMPUTACION

PRESENTA:
GONZALEZ MONDRAGON, ARACELI

1997

28
2e1.

UNIVERSIDAD NACIONAL AVENMA DE MEXICO

0 0 4 7 8 2

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES "ACATLÁN"

COORDINACIÓN DEL PROGRAMA DE MATEMÁTICAS APLICADAS Y COMPUTACIÓN

SRITA. ARACELI GONZÁLEZ MONDRAGON
Alumna de la carrera de Matemáticas Aplicadas y Computación
Presente. '97 JUN 25 PM 3 24

De acuerdo a su solicitud presentada con fecha 30 de septiembre de 1996, me complace informarle que esta Coordinación tuvo a bien asignarle el siguiente tema de tesina: "Auditoria Informatica", el cual desarrollará como sigue:

Introducción
I. Conceptos generales
II. Funciones del área de Auditoria Informática
III.Metodología propuesta para la Auditoria Informática
IV.Plan de contingencias
Conclusiones

Asimismo fue designado como Asesor de la Tesina al Lic. Juan Carlos Rendón Aguilar, profesor de esta Escuela.

Ruego a usted tomar nota que en cumplimiento de lo especificado en la Ley de Profesiones, deberán prestar servicio social durante un tiempo mínimo de seis meses como requisito básico para sustentar el examen profesional, así como de la disposición de la Coordinación de la Administración Escolar en el sentido de que se imprime en lugar visible de los ejemplares de la tesina el título del trabajo realizado. Esta comunicación deberá imprimirse en el interior de la tesina.

Atentamente
"POR MI RAZA HABLARÁ EL ESPIRITU"
Acatlán, Edo. de Méx., a 9 de mayo de 1997.

LIC. BEATRIZ TRUEBA RÍOS
Jefe del Programa de M.A.C.

DEDICATORIA

A DIOS

A Tí Señor, porque eres el motivo que me hace ser mejor cada día.

A MIS PADRES

Dedico este trabajo con todo mi amor especialmente a mis padres, como una forma de agradecimiento por todos sus esfuerzos y por el cariño y apoyo que siempre me han brindado.

A MIS HERMANOS Y AMIGOS

Por su firme apoyo en cada momento de mi vida, que me permite sentirme alentada a seguir superándome.

INDICE

CAPITULO III

METODOLOGIA PROPUESTA PARA LA AUDITORIA INFORMATICA

CAPITULO IV

PLAN DE CONTINGENCIAS

INTRODUCCION

A lo largo de la historia, las sociedades han buscado instrumentos para aumentar la productividad, reducir costos e incrementar la calidad de los bienes y servicios, que en conjunto han caracterizado la vida económica y social del hombre.

Uno de esos instrumentos son las computadoras y las llamadas tecnologías de la información, que a pesar de su corta existencia, están transformando las estructuras mundiales de producción y de comercialización, así como la prestación de servicios. A estos impactos en la esfera económica hay que agregar otros que abarcan innumerables aspectos de la vida humana, tanto en las dimensiones social y política, como en el ámbito cultural.

En México, desde tiempo atrás se ha reconocido que debemos adoptar una actitud responsable y activa frente a las oportunidades que nos brindan las tecnologías de la información.

Es común sostener que el mundo vive una segunda revolución industrial, derivada del desarrollo convergente de las tecnologías de la computación, la información, la microelectrónica y las telecomunicaciones. Ninguna industria ha tenido un avance tecnológico que pueda compararse con el vertiginoso desarrollo de la informática, tanto en la reducción de costos como en el aumento real y potencial de la eficiencia a través de sus aplicaciones.

Con la incorporación de las tecnologías de la información en el diseño y el control de la producción, los países industrializados tienden aceleradamente hacia una automatización generalizada, en la búsqueda de varios propósitos: una alza sustancial de la productividad; el mejoramiento de la calidad de los productos; un control más seguro de los procesos; la disminución de los costos y la obtención simultánea de un incremento en la capacidad de innovación; y, una disminución del valor relativo de la mano de obra frente al de la tecnología de producción. A estas ventajas se suma, además, que el uso adecuado de la tecnología informática dentro de la organización asegure sus objetivos de apoyo a la misión de la empresa y tienda al ahorro de tiempo, energéticos y materias primas, lo que evita desperdicios y problemas asociados con tecnologías menos avanzadas.

Las instituciones educativas y de investigación que están a la vanguardia, también sustentan gran parte de su producción, almacenamiento, comunicación y uso de datos en sistemas informáticos. Algo similar sucede en el campo del desarrollo científico y tecnológico, que hace ya tiempo depende, tanto del acceso a la información a través de redes, como de la capacidad de simular y diseñar procesos computacionales que contribuyan a la predicción, manejo y explicación de todo tipo de fenómenos.

Asimismo, la eficiencia y la productividad de las organizaciones de todo tipo de servicios -públicos y privados- dependen cada día más de los soportes informáticos. Este apoyo hace viable la descentralización y modernización de las estructuras de administración para satisfacer más adecuadamente las demandas básicas de los clientes, en la medida que permiten que la información necesaria se encuentre distribuida en el lugar y en el momento adecuado para efectuar trámites y para tomar las decisiones pertinentes al nivel requerido.

Si bien el uso de sistemas de información modernos están incorporados a todas las áreas mencionadas, en un futuro cercano contribuirán sin duda a acelerar aún más esta revolución tecnológica. En efecto, la informática no sólo está transformando las estructuras mundiales de producción y comercialización, sino que se está imponiendo inevitablemente a la vida cotidiana porque es susceptible de ser incorporada a prácticamente cualquier actividad humana.

Estos importantes cambios han afectado la necesidad de información por parte de los directivos para planear, evaluar y controlar las operaciones de las organizaciones, así como para tomar decisiones oportunas. Este crecimiento en la necesidad de manejar información ha sido paralelo al crecimiento del procesamiento de datos.

Con la introducción de nuevas tecnologías y con esta creciente dependencia del procesamiento de datos, nuevas técnicas y procedimientos de auditoría y control son requeridos y están siendo desarrollados para ser aplicados en esta área, sin dejar de existir la marcada interrelación que guarda la auditoría y el control, dado que los controles en el ambiente de procesamiento de datos gobiernan el proceso de transacciones, el mantenimiento de registros, los reportes y el ambiente de seguridad, mientras que la auditoría evalúa y verifica esos controles y los resultados.

El objetivo principal de la auditoría informática, es el de auxiliar a la gerencia de la empresa y a la organización en general, en el efectivo desempeño de los sistemas informáticos, así como en el manejo adecuado de los datos, la explotación correcta de la computadora y la satisfacción de las necesidades que deba cumplir cada sistema.

Dada la impresionante transformación que se está dando en la función de la informática, se requiere hacer una utilización cada vez más cuidadosa y selectiva de esta tecnología, con base en criterios de conveniencia, viabilidad y economía.

Por otro lado, es importante determinar que tan dependiente es una organización en relación con sus sistemas informáticos. La necesidad de la auditoría informática surge desde el momento en que se cuenta con sistemas de información parcial o totalmente computarizados que tienen alguna trascendencia para la organización.

Un aspecto de suma importancia, es que no debe considerarse a la función informática o a los recursos informáticos como un ente aislado dentro de una organización, lo cual sucede muchas veces. Esto es, se realiza una auditoría dentro del área de informática para revisar sus controles, sus procedimientos, etc., y se olvidan de la relación que existe entre la función informática y su organización, así como de todo el medio que lo rodea.

Es fundamental determinar el potencial de los sistemas de información dentro de la organización. El primer paso es considerar la misión informática dentro de un contexto de organización: identificar las relaciones que existen, los servicios que brinda a las demás áreas de la organización; de aquí partimos para determinar el nivel de dependencia, que tan importante es la función informática o cuales son los alcances que podría tener en una empresa.

Posteriormente, se efectúa la revisión de la infraestructura informática, abarcando toda la estructura organizacional y administrativa de la función, verificando que exista una buena organización y adecuados canales de comunicación, que estén bien definidas las tareas, que haya controles presupuestales, etc.

El proceso de auditoría informática se puede concebir como la fuerza que ayuda a las organizaciones a lograr sus objetivos, minimizando la materialización de debilidades y riesgos, además de redituar en el logro de la salvaguarda de activos, la integridad de datos y la eficiencia y eficacia de los sistemas de información.

La auditoría en informática es un área de estudio relativamente nueva en nuestro país, por lo que la presente investigación está dirigida a todas aquellas personas interesadas en el tema, pero principalmente a quienes sin experiencia previa, tienen en un momento dado que realizar las funciones que ella implica, fungiendo como una guía básica que les permitirá adentrarse en el ámbito de la auditoría, para desarrollar entonces una metodología propia que se adecue a las situaciones que se presentan cotidianamente, contribuyendo así a la evolución de esta disciplina.

Por tal razón, esta investigación ha sido desarrollada con la finalidad de proporcionar al lector conceptos y lineamientos actualizados que son de utilidad para comprender la importancia de esta área, la cual surge por la necesidad de contar con una función encargada de vigilar el entorno computacional.

Por otra parte, se pretende aportar una obra de consulta para el estudiante, tanto del ámbito informático, como de todo aquel que de alguna manera se relacione con éste, ya que actualmente el material bibliográfico a su alcance es escaso.

Teniendo como base los anteriores planteamientos, esta investigación se desarrolló en cuatro capítulos cuyo contenido es el siguiente:

El capítulo I introduce al lector a los Conceptos Generales que serán tratados y mencionados a lo largo de la investigación, con objeto de formar un criterio y puntos de vista homogéneos; así también, se presentan definiciones esenciales de una auditoría informática, se resalta la importancia que ésta tiene para las organizaciones de nuestros días y los objetivos que persigue.

Asimismo, se propone una ubicación jerárquica del área mencionada en una organización, el perfil idóneo del auditor en informática y se hace mención de otros enfoques que se le pueden dar a la auditoría.

Por otra parte, se describe la práctica de la auditoría informática incluyendo la utilización de técnicas y la planeación de procedimientos.

En el capítulo II se presenta un estudio de las tres grandes funciones de la auditoría, como son: la Auditoría a la Gestión Informática, a los Sistemas en Desarrollo, así como a los Sistemas en Operación.

El capítulo III propone una metodología para una auditoría informática, partiendo desde su preparación, técnicas que se utilizarán, investigación preliminar, elaboración de cuestionarios y entrevistas, recopilación de documentos, análisis de la información, hasta el informe final.

Finalmente, el último capítulo resalta la creciente necesidad de contar con planes de contingencia en las organizaciones, ya que éstas dependen cada vez más de los sistemas de información para sus operaciones críticas y para aumentar el uso de las telecomunicaciones.

CAPITULO I

CONCEPTOS GENERALES

Para definir las funciones y responsabilidades de la auditoría informática, es conveniente referirse al papel que juega la auditoría en general dentro de un esquema de organización.

"Una organización nace en el momento en el que se establecen procedimientos explícitos para coordinar las actividades de un grupo con miras a la consecución de objetivos específicos".[1]

Así, una organización como tal, parte de la definición de sus objetivos, los cuales son revisados y actualizados periódicamente de acuerdo con las características del entorno y de la propia organización en sus aspectos internos.

Una vez definidos estos objetivos, se lleva a cabo la especificación y/o actualización del plan de acción para el logro de los resultados que se deben alcanzar.

1.1 Auditoría

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

Tradicionalmente este término ha sido mal empleado, ya que se considera como una evaluación, cuyo único fin es detectar errores y señalar fallas. Sin embargo, dicho concepto tiene un significado más amplio, que requiere del ejercicio de un juicio profesional sólido y maduro para juzgar los procedimientos y lineamientos que deben seguirse para evaluar los resultados obtenidos.

---

[1] Colegio de Licenciados en Ciencias Políticas y Administración Pública, Diccionario de Política y Administración Pública, p.43

Estos conceptos nos hacen pensar en las siguientes ideas:

a) Juicio profesional. El auditor obtiene los elementos de juicio necesarios para fundamentar de una manera clara y objetiva su opinión, con un criterio independiente, cumpliendo así con los lineamientos inherentes a su profesión.

b) Procedimientos y lineamientos. Mediante la aplicación de métodos de investigación, técnicas formales y pruebas, el auditor puede cerciorarse de la autenticidad y razonabilidad de los hechos e información.

c) El objetivo final de la actuación del auditor será el de emitir una opinión sobre la efectividad y confiabilidad de la información y área bajo estudio.

Por otra parte, el Diccionario de la Lengua Española define la auditoría como:

"El examen de las operaciones financieras, administrativas y de otro tipo de una entidad pública o de una empresa, por especialistas ajenos a ellas, con objeto de evaluar la situación de las mismas".[2]

Con los elementos anteriores, entenderemos por auditoría a *la actividad profesional que implica el ejercicio de técnicas y procedimientos especializados, aplicables al tipo de revisión que deberá efectuarse con el objeto de evaluar y mejorar lo existente, detectar y corregir errores y proponer alternativas de solución en un informe que sirva de base para la toma de decisiones como resultado del trabajo realizado.*

1.1.1 Tipos de Auditoría

La auditoría, como cualquier disciplina, toma características diferente de acuerdo al campo de acción o área de aplicación en que se desenvuelve.

De acuerdo a las personas que la realizan, se puede clasificar en dos tipos de auditoría: auditoría externa o independiente y auditoría interna.

---

[2] Real Academia Española, Diccionario de la Lengua Española, p.142

Auditoría Externa

"Es la auditoría que se realiza a solicitud de las organizaciones, con el objeto de presentar una opinión profesional independiente acerca de la razonabilidad y confiabilidad de la información y los recursos a examinar, expresada bajo los principios y políticas de la misma." [3]

La labor de auditoría externa implica una competencia profesional singular, caracterizada por una serie de atributos tales como independencia, conocimientos especializados y dedicación al servicio.

El auditor externo está capacitado para brindar cualquier servicio que implique el examen de información, operaciones, procedimientos, actividades y proyecciones que necesiten de un juicio profesional independiente dentro de su marco de competencia.

Auditoría Interna

"Es una evaluación independiente de las operaciones realizadas por los empleados o funcionarios de la organización, con propósitos de control." [4]

La aucitoría interna es una función gerencial que mide y valora la eficacia de los controles, políticas y procedimientos definidos por la organización para que se cumplan de acuerdo a lo establecido.

Este tipo de auditoría es una actividad apreciativa, independiente de los sectores objeto de revisión, por lo tanto, reporta directamente a los máximos niveles de la organización. Tiene por objeto la revisión de las operaciones para servir de base a la administración, por este motivo, es un control que se describe como independiente puesto que mide y evalúa la eficacia de otros controles.

La auditoría interna deberá trabajar en forma separada a las operaciones de la organización.

---

[3] Slosse, Carlos, et al., Auditoría, Un Nuevo Enfoque Empresarial, p.8

[4] Ibid. p.17

Sus funciones incluyen:

- Revisión de las operaciones para verificar la autenticidad, exactitud y efectividad de acuerdo a las políticas y procedimientos establecidos por la organización.

- Comprobación de la confiabilidad de datos de la administración, producidos dentro de la organización.

- Evaluación de la calidad de desempeño en la ejecución de las responsabilidades asignadas.

- Revisión de los procedimientos para conocer si estos fueron aplicados en forma consistente con las normas establecidas.

Como conclusión, podemos decir que estos dos tipos de auditoría deberán trabajar en forma coordinada, ya que el alcance de revisión del auditor externo es inferior al del auditor interno, en razón a su tiempo de permanencia en la organización, por lo cual el primero, se deberá apoyar en el trabajo del cuerpo de auditoría de la organización.

1.2 Informática

Actualmente no existe una definición de informática que tenga reconocimiento universal, por lo tanto, propondremos una que se apegue lo más posible a las necesidades de esta investigación.

El concepto informática tiene su raíz en la palabra francesa "informatique", neologismo utilizado para combinar las palabras *information y automatique* (información y automática), para indicar que la informática es la ciencia del tratamiento racional, particularmente por máquinas automáticas, de la información considerada como el soporte de conocimientos y comunicaciones, dentro de los ámbitos técnicos, económicos y sociales.

"En 1973 se publica en México una de las primeras obras de habla hispana en la que se pretende presentar una concepción de informática. En este trabajo se plantea a la informática como el estudio que define las relaciones entre medios (equipo), los datos y la información necesaria en la toma de decisiones, desde el punto de vista de un sistema integrado".[5]

Según Mathelot, "... la informática puede ser definida como la ciencia del tratamiento lógico y automático del soporte de conocimientos y comunicaciones humanas, a saber, la información".[6] Lo cual quiere decir que la informática comprende todo a la vez y de manera indisoluble los medios de tratamiento, su funcionamiento y el estudio de los ámbitos de aplicación.

En esta investigación, entenderemos a la informática como *el tratamiento automático de la información*.

1.3 Control Interno

Un concepto actualizado de lo que es el control interno lo expresó la Comisión para la Prevención del Fraude, creada en 1985 por el Comité de Organizaciones Patrocinadoras, en el cual indica:

"Control interno es un proceso llevado a cabo por el Consejo de Administración, la Gerencia y otro personal de la organización que está diseñado para proporcionar una garantía razonable sobre el logro de objetivos en una o más de las siguientes categorías:

- Efectividad y eficiencia de las operaciones (incluyendo las metas de rendimiento y rentabilidad).

- Contabilidad de la información financiera (tanto la difundida interna como externamente, incluyendo la prevención de informes financieros fraudulentos).

- Cumplimiento con las leyes, reglamentos, normas y políticas."[7]

---

5 Lambarri Valencia, Alejandro, Curso de Auditoría Informática, p.26

6 Mathelot, Pierre, L'informatique, que sais-je, p.7

7 Tradeway Commission, Reporte Final 1992, p.41

Entenderemos como control interno *cualquier acción que se lleve a cabo para propiciar el logro eficaz y eficiente de objetivos de la organización*, esto con la intención de no restringir el concepto al ámbito financiero, además de darle sencillez y amplitud.

Luego entonces, se puede afirmar que uno de los propósitos fundamentales de la auditoría informática será el determinar el riesgo existente en la organización y promover la optimización permanente del control o su propia implantación.

1.4 Auditoría Informática

Los autores Mair, Wood y Davis describen la auditoría informática como la verificación de los controles en tres áreas de la organización: [6]

- Las **aplicaciones** abarcan todas las funciones de información de la empresa, donde la computadora interviene en los procesos. Los sistemas de aplicación involucran uno o más departamentos de la organización, así como de operaciones computacionales y de desarrollo de sistemas.

- El **desarrollo de sistemas** incluye las actividades de los analistas de sistemas y programadores, quienes desarrollan y modifican archivos de aplicación, programas de computación y otros procedimientos.

- La **instalación del proceso de información** comprende todas las actividades involucradas en el equipo computacional y archivos de datos. Esto incluye las operaciones computacionales, la librería de archivos computacionales, el equipo de entrada y salida de datos y la distribución de información. Las preocupaciones con respecto a los trabajos que realiza la computadora, no se eliminan sencillamente porque las lleve a cabo un tercero -un centro de servicio (service bureau).

  El empleo de un service bureau independiente puede conceder valiosos ahorros, así como eliminar preocupaciones del usuario en actividades concernientes a la eficiencia operacional, pero nada lo relevará de su responsabilidad en la salvaguarda de los activos y la confiabilidad de la información.

---

[6] Vid. Mair, William C.; Wood, Donald R., et al., Computer Control & Audit, p.17

Según Weber la auditoría "... es el proceso de recolección y evaluación de evidencia, para determinar si un sistema automatizado: salvaguarda activos, mantiene la integridad de datos, alcanza las metas organizacionales efectivamente y consume recursos eficientemente". [9]

Para efectos de esta investigación, conceptualizaremos el término de auditoría informática como:

> *El examen y validación de los controles, técnicas y procedimientos utilizados e implantados en el centro de cómputo, sistemas en operación y bajo desarrollo, a fin de verificar que los objetivos de salvaguarda de activos, continuidad de servicio, confiabilidad, seguridad, integridad y consistencia en la información, se están cumpliendo en forma satisfactoria y oportuna, y de acuerdo a los objetivos y políticas establecidas por la organización.*

1.4.1 Objetivos de la Auditoría Informática

De acuerdo a la Asociación Mexicana de Auditores en Informática, fundada en 1976 con la finalidad de promover la capacitación de los asociados para desarrollar sus habilidades en el campo de la auditoría, control y seguridad en los sistemas de información, los objetivos de la auditoría informática se pueden resumir como se plantea a continuación: [10]

- Ayudar a los miembros de la dirección en el desempeño efectivo de sus responsabilidades, proporcionándoles análisis, estimaciones, evaluaciones, recomendaciones y comentarios pertinentes concernientes a las actividades revisadas.

- El auditor se preocupa por cualquier actividad del negocio donde pueda ser útil para ayudar a la administración. Esto implica ir más allá de la contabilidad y los registros financieros para obtener un total entendimiento de las operaciones que está revisando. El logro de esto, involucra actividades como:

---

[9] Weber, Ron, EDP Auditing, Conceptual Foundations and Practice, pp.9-11

[10] Cfr. Historia de la Asociación Mexicana de Auditores en Informática, A.C., p.3

a) Disminuir los riesgos de las operaciones de la organización, relacionados con el procesamiento de datos, tanto en el desarrollo y operación de sistemas como en las instalaciones de cómputo.

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

c) Participar en el proceso de desarrollo de sistemas, con objeto de vigilar la adecuada administración de proyectos y que los controles necesarios sean instrumentados.

d) Supervisar las funciones del área de sistemas para evaluar la confidencialidad y seguridad de los sistemas de información en operación.

e) Evaluar las medidas de seguridad implantadas en las áreas de procesamiento de datos, para proteger las instalaciones, los equipos y la información contra siniestros.

f) Evaluar las fortalezas y debilidades del área que se audita para informar del estado de los controles al analizar las evidencias de auditoría.

Por otro lado, el uso de la computadora para evaluar la confiabilidad del sistema de procesamiento de datos y determinar la calidad de la información generada por el sistema, parece proporcionar al auditor la oportunidad de llevar a cabo una auditoría más selectiva y de mayor penetración, respecto a las actividades y procesos que implica un gran volumen de transacciones.

Mediante una revisión adecuada del sistema de procesamiento electrónico de datos y el uso de datos bien diseñados para comprobación, el auditor puede lograr un mejor conocimiento de los procedimientos y controles del ente auditado. Al crear programas de auditoría por computadora, el auditor puede cubrir un área más extensa de la actividad tanto financiera como operacional, y puede utilizar recursos humanos para analizar campos de problema de evaluación en las operaciones del ente. Tal método incrementa la aptitud del auditor para rendir óptimo servicio.

La auditoría tradicional se ha preocupado históricamente por cumplir con los requisitos de reglamento y de custodia, poniendo énfasis en los controles contables. Sin embargo, con el advenimiento de la tecnología de sistemas de información, ha crecido la necesidad de una evaluación sobre lo adecuado de la información administrativa, así como su exactitud. En adición a la necesidad de auditar los registros financieros de una organización, ha evolucionado lo imperativo, que es auditar también los instrumentos de que se vale la dirección para determinar la pertinencia de la información que se le suministra para la planeación estratégica, el control administrativo y las actividades operativas.

En la presente investigación, sugerimos que el examen de auditoría tenga como objetivo: *crear un mejor entendimiento de los requisitos de información de la organización y evaluar lo adecuado de los sistemas de información de la entidad para satisfacer tales requisitos*. En virtud de tal objetivo, no sólo se evaluaría la función de vigilancia de la dirección o la contabilidad, como lo reflejan los estados financieros, sino también lo adecuado de la información administrativa para la planeación, control y propósitos de toma de decisiones.

Este nuevo enfoque ofrece muchas implicaciones y conduce a oportunidades y problemas de auditoría significativamente ampliadas, que nos plantean puntos de reflexión, preocupaciones y retos, como los son:

1. La cada vez mayor delegación de funciones a personal no preparado, obliga a replantearse cuestionamientos en relación con la incorporación de estructuras organizacionales, políticas y procedimientos de control, suficientemente fuertes para garantizar un grado de riesgo tolerable en cuanto a:

   - La salvaguarda (custodia) de los activos: materiales, tecnológicos y humanos.
   - La generación de información para la toma de decisiones a todos los niveles de la organización.
   - La promoción de la eficiencia operativa.
   - La adhesión a la normatividad interna y externa, sujeta a canales de comunicación adecuados y constantes.

2. La necesidad de elevar la calidad del servicio e innovar, para estar en condiciones de enfrentar las cambiantes necesidades de la sociedad.

3. La conveniencia de aprovechar las enormes ventajas científicas y tecnológicas que nos ofrece el mundo actual en todos los campos, como en el caso de las computadoras, las comunicaciones y el desarrollo del gigantesco potencial humano.

1.4.2 Importancia de la Auditoría Informática

Estudios realizados por el Instituto de Investigaciones de Standfor, basados en encuestas y entrevistas orientadas a directivos de varias empresas, revelaron necesidades de atención de la alta gerencia y necesidades de inversión adecuada de dinero, staff y manejo de tiempo para asegurar el desempeño correcto de las funciones de auditoría y control para cada sistema de procesamiento de información. [11]

Las conclusiones obtenidas de este estudio fueron:

- La responsabilidad primaria de los controles internos reside en la alta gerencia, mientras que la operacional, para la completa y precisa información basada en sistemas de cómputo, reside en los usuarios.

- Existe una necesidad de incrementar los controles debido a que una inadecuada atención ha sido dada a la importancia de los controles internos en el ambiente de procesamiento de datos.

- Los auditores internos deben participar en el proceso de desarrollo de sistemas para asegurar que los principios de auditoría y control sean incorporados en el nuevo sistema de información para computadora.

- La verificación de controles debe ocurrir antes y después de instalar un sistema de cómputo.

- Como resultado de la creciente complejidad y uso de sistemas de información basados en computadora, existe la necesidad de mayor auditoría interna orientada al ambiente de procesamiento de datos.

---

[11] Cfr. Higley Russell, Susan; Eason Tom, S ; Fitzgerald, J. M., Data Processing Control Practices Report, p.78

- Existe una importante necesidad de desarrollar un staff de auditores en el área de procesamiento de datos con gente de sistemas, ya que tienen suficiente conocimiento y experiencia para efectuar efectivamente el proceso de auditoría.

- Son necesarias nuevas técnicas y herramientas para llevar a cabo la función de auditoría informática, ya que de las existentes son pocas las que se adecuan a las necesidades del auditor en informática.

- Muchas organizaciones no están evaluando adecuadamente sus funciones de auditoría y control en el área de procesamiento de datos. La alta gerencia debe iniciar una evaluación periódica de sus programas de auditoría y control.

1.4.3 Perfil del Auditor en Informática

El aspecto fundamental en la definición del perfil más adecuado para llevar a cabo las funciones de auditoría informática, es la controversia entre personal con perfil de informática, al que se le capacita en funciones de control; o el perfil de auditor, al que se le da capacitación en tecnología de cómputo. [12]

Ahora bien, por perfil de un profesional, hemos de entender las características, aptitudes o requisitos mínimos que debe reunir una persona para ejercer una profesión. [13]

El perfil profesional se integra por características generales que se encuentran representadas por los requisitos intelectuales y personales que ha de poseer un auditor en informática, con independencia del área en la que se desenvuelva, tales como:

- Capacidad e interes intelectual, es decir, disposición y aptitudes para captar, comprender, evaluar y aplicar los conocimientos.

---

[12] Ctr. Colegio de Contadores Públicos de México., Diferentes Enfoques de Auditoría en Informática, p.13

[13] Vid. López Elizondo, La Profesión Contable, Selección y Desarrollo, p.104

- Habilidad para evaluar en forma objetiva e independiente. Esto implica un conocimiento funcional de los estándares aceptados en el área de procesamiento electrónico de información y la habilidad para comparar operaciones, funciones y procedimientos en aquellos estándares.

- Aptitud para reconocer rápidamente problemas claves. Una función importante de la auditoría es la de identificar problemas y deficiencias fundamentales, así como el sugerir medidas adecuadas de corrección.

- Capacidad para comunicarse eficazmente. Una cantidad considerable de información es la que se maneja, por lo que es necesario comprenderla para transmitirla correcta y oportunamente al personal correspondiente.

Estas características le servirán para efectuar las siguientes funciones

Funciones del Auditor en Informática.-

1. Sistemas en Desarrollo

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

2. Sistemas Automatizados en Operación

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

3. Administración y Seguridad de Centros de Procesamiento

   - Calendarización y control de producción
   - Controles de acceso y seguridad física
   - Cintoteca, respaldos y software del sistema
   - Procedimientos de respaldo y recuperación
   - Planes de contingencia

4. Sistemas Avanzados de Cómputo

- Sistemas de base de datos
- Sistemas basados en procesamiento distribuido
- Redes de comunicación de datos

5. Salvaguarda de los Activos de Cómputo y Mantenimiento

- Cobertura de seguros e información de activos actualizada
- Programas de mantenimiento preventivo, directivo y correctivo

6. Aspectos Generales de Sistemas

- Cumplimiento y actualización del plan de sistemas
- Usos y aprovechamiento de recursos informáticos
- Administración del área

7. Apoyo a las Areas de Auditoría Informática

- Usos y aprovechamiento de recursos informáticos centralizados.
- Automatización de los procedimientos de auditoría
- Automatización de las funciones administrativas de auditoría
- Auditoría con y a través de la computadora

1.4.4 Ubicación Jerárquica del Area

Cuando nos referimos a la ubicación que debe ocupar el area de auditoría informática, nos encontramos ante una situación polémica, ya que dependerá del tamaño, contexto y complejidad de la organización, así como del nivel de automatización de la misma.

Considerando lo anterior, dicha área debe estar ubicada de manera separada a las áreas usuarias, al área de sistemas, así como de la Gerencia y Dirección donde se realiza la toma de decisiones. Esto permite al área poder contar con autoridad propia y bien definida, a fin de realizar sus actividades y actuar con un criterio imparcial e independiente, para obtener como producto de sus funciones resultados objetivos.

1.5 Otros tipos de Auditoría

Si bien le hemos llamado Auditoría Informática a la materia en estudio para diferenciarla de la auditoría tradicional que se dedica al examen de información preferentemente financiera y en particular a los estados financieros, no se debe olvidar que al haber adoptado una definición más amplia de la auditoría, la cual se enfoca, bajo este concepto, a la revisión y examen sistemático de actividades que realiza personal independiente de la operación (dentro de éstas cae la informática), por lo tanto, es válido al hablar de auditoría, estar incluyendo la auditoría informática, la financiera, la de operaciones, etc. A continuación se mencionan algunos de los tipos de auditorías más usuales, de acuerdo con Ramírez y Valdez, con objeto de mostrar otros enfoques que se dan en esta materia:

"Auditoría Financiera.- Diseñada para verificar la precisión de las declaraciones contables y que estén preparadas de conformidad con los principios de contabilidad generalmente aceptados y congruentemente aplicados.

Auditoría de Operaciones.- Utilizaca para revisar y evaluar la eficiencia y economía de los métodos y procedimientos de la organización.

Auditoría Administrativa.- Tiene que ver con la evaluación de la forma en la que la administración está cumpliendo sus objetivos, desempeñando las funciones gerenciales de planeación, organización, dirección y control; logrando decisiones efectivas en el cumplimiento de los objetivos trazados por la organización.

Auditoría Tecnológica.- Se ubica como una especialidad de la auditoría administrativa, enfocada a evaluar la función de la tecnología (investigación, desarrollo e ingeniería), la función de producción, la función de personal y la función del sistema de información.

Auditoría Social.- Dedicada no sólo a informar de la participación de la organización en las actividades socialmente orientadas, sino también a determinar si alcanzó sus objetivos por actividad."[14]

---

[14] Ramírez Bustos, Juan y Valdez Hernández, Alfredo, Desarrollo Tecnológico, una Posibilidad al Alcance de su Empresa. p.102

1.6 Práctica de la Auditoría Informática

En un esfuerzo por relacionar los objetivos de la auditoría que hemos sugerido, con las tareas de auditoría que se requieren, encontraríamos de gran utilidad estructurar la discusión en términos de las principales fases de un examen de auditoría: la evaluación del sistema y la evaluación del resultado del sistema, pues con el objeto de llevar a cabo el examen de auditoría que esperamos, el auditor tiene que obtener suficiente material evidencial para:

- Determinar que existe un sistema que proporciona datos pertinentes y confiables para la planeación y control

- Determinar que este sistema produce resultados -es decir, planes, presupuestos, pronósticos, estados financieros, informes de control, etc.-, que son dignos de confianza y fáciles de entender por el usuario.

La clave para llevar a cabo estas tareas generales, es la evaluación del sistema de información del sujeto auditado, el cual es importante para poder apreciar aquellas áreas del sistema donde existen diferencias y donde podrían producirse mejoras.

Para obtener material evidencial suficiente para formar una opinión de auditoría sobre el sistema, el auditor lleva a cabo ciertos procedimientos específicos, usando una gran variedad de técnicas. Nuestra intención es clasificar los procedimientos específicos de auditoría, en tareas fundamentales de auditoría común a la mayoría de las aplicaciones pertinentes.

Al evaluar un sistema de información o de control interno, o cualquier otro sistema, el auditor ha de preocuparse más por efectuar un análisis de la estructura y diseño del sistema en sí, que por el examen intensivo de los documentos y registros producidos por tal sistema. Desde este punto de vista, cualquier examen de transacciones y registros, se diseña primordialmente para confirmar la existencia de procedimientos y su efectividad, para mejorar el entendimiento y elementos del sistema.

En la revisión y evaluación de los sistemas, el auditor debe seguir un proceso básicamente similar al que sigue el analista de sistemas al diseñar o implantar los sistemas; la diferencia estriba esencialmente en los objetivos y énfasis del procedimiento.

Para evaluar el sistema, el auditor lleva a cabo estas tareas:

1. Definir el sistema que está en función

2. Poner a prueba el sistema para confirmar la exactitud de su definición

3. Evaluar los puntos fuertes y débiles del sistema, a fin de determinar:

   - Procedimientos de auditoría adicionales que se requieran en áreas donde existe debilidad;

   - Recomendaciones para mejorar el sistema a la luz de las necesidades de información del ente.

Para entender inicialmente la estructura, elementos y propiedades del sistema, el auditor informático debe definir el sistema que desea evaluar. En la definición de sistemas, es importante especificar el propósito y restricciones del sistema bajo análisis. Los métodos clásicos, incluyendo diagramas de flujo y representaciones del ordenamiento que se usa, se han venido utilizando en la definición de sistemas. Estos métodos están diseñados para describir un sistema con detalle suficiente y con bastante eficiencia analítica, para proporcionar al auditor una clara descripción de la estructura y componentes del sistema sobre la que pueda trabajar. La descripción debe ser capaz de especificar lo que hace el sistema y que resultado debe tener lugar, dados los insumos fijados (el proceso electrónico de los datos).

En virtud de que por lo general está revisando un sistema que ya se definió y describió y para el que se cuenta con documentación relativa, el auditor comienza por hacer su evaluación del sistema, revisando la documentación pertinente al procedimiento, haciendo preguntas al personal responsable del sistema y observando el sistema en funcionamiento. De esta manera, el proceso debe dar al auditor una definición y descripción provisional del sistema. Para tener mayor seguridad de que la definición provisional es razonablemente buena, o definitivamente mala, así como para observar los puntos fuertes y débiles del sistema, debe efectuarse un análisis adicional.

Para confirmar la definición del sistema y determinar la efectividad de los elementos que los componen, el auditor debe introducir pruebas o procedimientos de diagnóstico.

Específicamente, las razones para efectuar pruebas, son:

- ¿Cómo funciona el sistema?
- ¿Funciona en la forma definida por el ente auditado?
- ¿Es susceptible de mejora?

El propósito de poner a prueba el sistema, es obtener cierta evidencia de que el sistema en función corresponde a la definición que de él hizo el auditor y determinar si los procedimientos que se suponen están en efecto, en verdad lo están. La finalidad no es determinar si los procedimientos están en vigor y funcionando una aceptable proporción de tiempo, por lo tanto, será suficiente un número limitado de pruebas de cada tipo de transacciones importantes en el sistema. En vista de los objetivos, deben emprenderse algunos puntos específicos en apoyo de la prueba limitada.

En primer lugar, aun cuando el auditor esté limitando sus pruebas, no las está limitando a una pequeña porción del sistema que se está revisando, en realidad, está poniendo a prueba unas cuantas transacciones de cada tipo que se procesan de manera distinta.

En segundo lugar, en este momento del análisis del sistema, el auditor no está tratando de sacar ninguna inferencia estadística respecto a la población de todas las transacciones de cierto tipo. No está tratando de probar que los errores nunca ocurrieron, sino meramente de establecer cuál es el sistema en operación.

En tercer lugar, puesto que está tratando de hacer que la forma en que él entiende el sistema y su evaluación sea una base para confiar en él y para la determinación del grado resultante de pruebas a que deben restringirse los procedimientos de auditoría, la investigación del auditor, que requiere pruebas extensas, debe llevarse a cabo después de que se ha evaluado el sistema. Cuando un procedimiento es obviamente débil, la repetida verificación de sus detalles tiene poco valor para determinar cual es el sistema y cuales sus puntos débiles y fuertes. Una vez que entiende cual es el sistema y ha evaluado sus puntos débiles y fuertes, puede entonces decidir efectuar pruebas adicionales en áreas donde el sistema no sea efectivo. Pero en esta etapa, su objetivo no está en entender y poner confianza en el sistema, sino en hacer evaluaciones basadas en sus pruebas.

Dado el objetivo de la auditoría -evaluar la aptitud del sistema de información de la entidad para satisfacer sus necesidades-, debemos dirigir nuestra atención a los medios para lograrlo.

Es claro que para el desempeño de la auditoría, se necesitan normas, tanto de método como de evaluación. Las normas de método se refieren a la forma en que se formula el entendimiento que se necesita de la organización y su sistema de información, mientras que las normas de evaluación, son para formarse un juicio respecto a lo adecuado del sistema de información de la entidad y sus varios resultados.

La evaluación de los sistemas se auxilia de diferentes herramientas, y una de estas puede ser la utilización de los sistemas electrónicos. Para poder evaluar un sistema de información es necesario conocerlo y controlarlo desde su inicio, siguiendo su proceso que puede ser manual, mecánico, electrónico o bien la combinación de estos, hasta llegar a su almacenamiento, respaldos, seguridad y eficiencia en el uso de la información que proporcionan. No basta, pues, conocer una parte del sistema como pueden ser los equipos de cómputo, que tan sólo vienen a ser una herramienta dentro de un sistema total de información. Sin embargo, en la presente investigación se hace énfasis en los procedimientos de auditoría a los centros de cómputo y áreas de informática, por ser los que requieren de mayor instrumentación.

Uno de los problemas más frecuentes en estas áreas, es la falta de una adecuada organización que permita avanzar al ritmo de las exigencias de las organizaciones. A esto hay que agregar la situación que presentan los nuevos equipos de cómputo en cuanto a la posibilidad de uso de bases de datos, redes y de información de gran capacidad.

Con objeto de establecer una efectiva función de auditoría informática, la organización ha de seleccionar al personal de esta área que cuente con una buena idea de los principios de auditoría y suficiente aptitud y conocimiento en el campo de procesamiento electrónico de datos, de acuerdo a los siguientes objetivos:

- Crear nuevas técnicas de auditoría computarizada y, siempre que ello fuera posible, incorporarlas en el sistema.

- Crear requisitos de control y técnicas para lograr que el personal de diseño de sistemas dé énfasis a la necesidad de un adecuado sistema de control.

- Evaluar la efectividad del sistema de control, cuando todavía se halle en el proceso de diseño.

- Evaluar todas las demás áreas, como pruebas de sistema y conversiones, donde los controles son esenciales.

El proceso de auditoría debe evaluar para mejorar lo existente, corregir errores y proponer alternativas de solución, así como recomendar mejoras operativas. La auditoría no está orientada a descubrir fraudes; sin embargo, el auditor debe estar consciente de que al practicar su examen podría encontrar alguno y que éste afectaría su opinión.

En el momento que se están elaborando los sistemas, el auditor interno debe participar en las siguientes etapas:

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

- Revisar la aplicación de los sistemas y de los controles, tanto con el usuario como en el centro de cómputo.

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

- Incorporar técnicas avanzadas de auditoría en los sistemas de cómputo.

1.6.1 Técnicas de Auditoría Asistidas por Computadora

En general, el auditor debe utilizar la computadora en la ejecución de la auditoría, ya que esta herramienta permitirá ampliar la cobertura del examen, reduciendo el tiempo/costo de las pruebas y procedimientos de muestreo, que de otra manera tendrían que efectuarse manualmente. Además, el empleo de la computadora por el auditor le permite familiarizarse con la operación del equipo en el centro de cómputo de la organización.

El empleo de la computadora en la auditoría, constituye una herramienta que facilita la realización de actividades como:

- Verificación de cifras totales y cálculos para comprobar la exactitud de los reportes de salida producidos por el área de informática.

- Pruebas de riesgos de los archivos para verificar la consistencia lógica, validación de condiciones y razonabilidad de los montos de las operaciones.

- Clasificación de datos y análisis de la ejecución de procedimientos.

- Selección e impresión de datos mediante técnicas de muestreo y confirmaciones.

- Simulación en forma independiente del proceso de transacciones para verificar la conexión y consistencia de los programas de computadora.

- Manejo de paquetes de auditoría; por ejemplo, paquetes provenientes de fabricantes de equipos, firmas de contadores públicos o compañías de software.

- Utilización de programas de auditoría desarrollados por proveedores de equipo, que verifican el empleo de la computadora o miden la eficiencia de los programas, su operación o ambas cosas.

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

- Mantener el control básico sobre los programas que se encuentren catalogados en el sistema y llevar a cabo protecciones apropiadas.

- Observar directamente el procesamiento de la aplicación de auditoría.

- Desarrollar programas independientes de control que monitoreen el procesamiento del programa de auditoría.

- Mantener el control sobre las especificaciones de los programas, documentación y comandos de control.

- Controlar la integridad de los archivos que se están procesando y las salidas generadas.

Utilización de Paquetes Comerciales de Auditoría.-

Paquete de auditoría es el término empleado para un conjunto de programas que tienen la capacidad de procesar uno o varios archivos de datos en medios magnéticos, funcionando bajo el control de parámetros definidos y aplicados por el auditor.

Esta es una técnica usada por los auditores informáticos, ya que permite analizar uno a más archivos de un sistema computarizado. Está orientada a probar datos, sin embargo poco ayuda a probar la lógica de los programas de cómputo, únicamente lo que pueda deducirse de los resultados al probar archivos de datos.

Estos programas han sido desarrollados por diferentes proveedores y por firmas de contadores o consultores, pueden ser adquiridos con el propósito de que el auditor pueda obtener, de una manera rápida y sencilla, la evidencia suficiente y competente que requiera el caso, siendo su empleo fácil y menos costoso que programas desarrollados a la medida.

Históricamente este tipo de software ha operado en modo "batch"[15], pero debido a la rápida expansión de sistemas computarizados operando "en línea"[16], recientemente los paquetes de auditoría permiten esta última ejecución.

Los archivos de datos pueden estar en diferentes dispositivos magnéticos, tales como cinta o disco, y en diferente organización, por ejemplo secuencial o de acceso directo. Los parámetros de entrada aplicados por el auditor especifican el tipo de archivo que se esté procesando, el proceso lógico a ser aplicado y el tipo de salida requerido (tipo de reporte). De esta manera, el auditor puede utilizar los paquetes de auditoría para probar un sistema computarizado en diferentes partes y de diversas formas.

Las funciones más comunes de los paquetes de auditoría son:

- Sumarización
- Sumas cruzadas
- Selección de datos y presentación detallada
- Ejecución de diversos cálculos matemáticos
- Formateo de reportes
- Comparación de 2 generaciones del mismo archivo de diferentes fechas, o dos archivos diferentes a la misma fecha con datos comunes.
- Clasificación
- Empleo de muestreo estadístico: determinación del tamaño de la muestra, selección de partidas a auditar y extrapolación de los resultados del muestreo al universo
- Comparación de diferentes archivos

---

[15] Método de procesamiento de datos en donde los trabajos se agrupan primero para después enviarse en forma secuencial a la computadora para su proceso.

[16] Archivos conectados electrónicamente al computador para efectos de acceso inmediato.

Algunos beneficios que podemos mencionar de utilizar paquetes comerciales de auditoría son los siguientes:

- De fácil uso para el auditor
- El paquete puede procesarse en hardware independiente
- Análisis de los archivos sin depender del personal de informática
- Uso efectivo de la computadora sin necesidad de entrenamiento intensivo y complejo
- Modificación de los procedimientos de auditoría para adaptarlos a los cambios operativos con esfuerzos reducidos
- Un paquete de auditoría puede utilizarse en la revisión de varios sistemas de información computarizados.

Desarrollo de Programas de Auditoría a la Medida de las Necesidades.-

En este concepto se encuentran todos los programas que son concebidos para realizar la revisión de una aplicación computarizada en particular, utilizando normalmente archivos de producción u operación.

Esta técnica está más difundida en empresas o instituciones que no están en posibilidades de adquirir un paquete o se trata de entidades cuyas actividades son unicas en el país y no está disponible un paquete comercial que satisfaga las necesidades de auditoría.

El empleo de esta técnica exige que se disponga de especialistas como parte del equipo de auditoría, aunque puede resultar costoso, ya que involucra la elaboración, prueba, ejecución y documentación de los programas de auditoría. sin embargo, es más flexible que la técnica anterior.

Los pasos a seguir en la aplicación de esta técnica son los siguientes:

1.- Definir las aplicaciones que requieren la intervención del auditor en informática, señalando los trabajos que se pretenden realizar.

2.- Recopilar los criterios y/o parámetros que se utilizarán en la selección de la muestra.

3.- Proporcionar especificaciones técnicas al programador, de todo un sistema y de cada programa, calendarizando las actividades. Se debe enfatizar el que se incorporen controles que garanticen la confiabilidad de los resultados a obtenerse.

4.- Desarrollar los programas de cómputo.

5.- Probar los programas con resultados de los archivos de producción

6.- Conciliar los resultados, cruzar las cifras de control.

7.- Evaluar los resultados de la prueba y sacar conclusiones.

1.6.2 Planeación de los Procedimientos de Auditoría

El propósito principal de la planeación de los procedimientos de auditoría, es incluir dentro de las aplicaciones, las facilidades que permitan realizar las actividades de auditoría de la manera más fluida.

Las características de los sistemas deben permitir una verificación independiente de:

- La actualización de los datos procesados por los sistemas;
- El correcto funcionamiento de los procedimientos ejecutados por el sistema; y,
- La utilización de procedimientos adecuados de control.

En resumen, el auditor debe tener la habilidad para revisar y probar la integridad de los sistemas.

Las actividades principales del auditor serán:

- Verificar los controles y procedimientos de la utilización y captura de los datos, su proceso y salidas de información, así como los programas que los generan. Es importante revisar los procedimientos para el mantenimiento de los programas y las modificaciones a los sistemas.

- Revisar las transacciones realizadas para asegurarse de que los archivos reflejan la situación actual.

- Revisar las transacciones y los archivos para detectar posibles desviaciones de las normas establecidas.

- Asegurarse de que las aplicaciones cumplan con los objetivos definidos en la planeación.

- Revisar todos los cambios hechos a los programas y sistemas para verificar la integridad de las aplicaciones.

1.6.3 Planeación de la Auditoría Informática

La auditoría informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistema o procedimiento específico, sino que además, habrá de evaluar los sistemas de información en general, desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información. Ello debe incluir los equipos de cómputo como la herramienta que permite obtener la información adecuada y la organización específica (departamento de cómputo, unidad de informática, departamento de procesos electrónicos, etc.) que hará posible el uso de los equipos de cómputo.

Para lograr los puntos antes señalados, necesita una evaluación administrativa del área de informática, que comprende:

- Objetivos del departamento, dirección o unidad.

- Metas, procedimientos, planes y políticas de procesos electrónicos estándares.

- Organización del área y su estructura orgánica.

- Funciones y niveles de autoridad y responsabilidad del área de procesos electrónicos.

- Integración de recursos materiales y técnicos.

- Dirección.
- Costos y controles presupuestales.
- Controles administrativos del área de procesos electrónicos.

Por otro lado, requiere hacer un análisis del sistema, donde se evaluarán las políticas, procedimientos y normas establecidas para llevar a cabo el análisis, teniendo especial cuidado en que los sistemas y su documentación sean acordes con las características y necesidades de la organización.

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

Asimismo, la evaluación del diseño lógico del sistema, en el cual el objetivo principal que se persigue es el de comparar lo planeado contra los resultados que se están obteniendo.

Como parte de este análisis, incluye la evaluación de los sistemas, procedimientos y uso de la información:

- Evaluación del desarrollo físico del sistema.
- Control de proyectos.
- Control de sistemas y programación.
- Instructivos y documentación.
- Formas de instrumentación.
- Seguridad física y lógica de los sistemas.
- Confidencialidad de los sistemas.

- Controles de mantenimiento y forma de respaldo de los sistemas.

- Utilización de los sistemas.

Así también, la evaluación del proceso de datos y equipos de cómputo, lo que comprende:

- Controles de los datos fuente y manejo de cifras de control. Con el establecimiento de esta medida, se busca tener un adecuado señalamiento de responsables de los datos con claves de acceso de acuerdo a niveles, por ejemplo, en el primer nivel se pueden hacer consultas, captura de datos, modificaciones y bajas; el segundo nivel es en el que se puede hacer lo mismo que el nivel anterior a excepción de modificaciones y bajas; y el tercer nivel es aquel en el que sólo se pueden hacer consultas.

- Control de operación. En él se establecen los instructivos de operación, procedimientos que debe seguir el operador en situaciones normales y anormales en el procesamiento, evitando errores, reprocesamientos y desperdicio de tiempo de máquina.

- Control de salida. Se establecen con el objeto de mantener una estrecha vigilancia en el manejo de los archivos y en general de todos los documentos de salida, especificando qué documentos son, quién los entrega, a quién se entregan, con qué periodicidad y la forma en que se salvaguarda la información no utilizada.

- Control de medios de almacenamiento masivos. El objetivo que se persigue al establecer dicho control, es el de realizar una adecuada administración de los dispositivos de almacenamiento masivo, para evitar la pérdida total o parcial de información, manteniéndolos perfectamente protegidos y estableciendo registros sistemáticos de la utilización de dichos archivos.

- Orden en el centro de cómputo. En este caso nos estamos refiriendo a la observancia de reglas establecidas relativas al orden y cuidado de la sala de máquinas, dispositivos del sistemas de cómputo y archivos magnéticos.

- Seguridad física y lógica. Con el objeto de verificar el cumplimiento del sistema de control interno, en materia de salvaguarda de los activos de la organización, el auditor llevará a cabo su revisión teniendo como puntos a desarrollar en esta fase la seguridad en el uso del equipo y de la información.

- Confidencialidad. Supervisa las funciones del área de sistemas para evaluar la confidencialidad y seguridad de los sistemas de información en operación.

- Respaldos. Con el objeto de mantener una adecuada administración de los dispositivos de almacenamiento, procedimientos de respaldo y recuperación.

1.6.3.1 Investigación Preliminar

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

A nivel Organizacional total:

- Objetivos a corto y largo plazo.
- Manual de organización.
- Antecedentes o historia del organismo.
- Políticas generales.

A nivel Organizacional del Area de Informática:

- Objetivos a corto y largo plazo.
- Manual de organización del área, incluyendo puestos, funciones, niveles jerárquicos y tramos de mando.
- Manual de políticas, reglamentos internos y lineamentos generales.

- Número de personas y puestos en el área.
- Procedimientos administrativos del área.
- Presupuestos y costos del área.

Recursos Materiales y Técnicos:

- Solicitar documentos sobre los equipos.
- Estudios de viabilidad.
- Número de equipos, localización y las características (de los equipos instalados, por instalar y programados).
- 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.
- Planes de expansión.
- Ubicación general de los equipos.
- Políticas de operación.
- Políticas de uso de los equipos.

Sistemas:

Descripción general de los sistemas instalados y de los que estén por instalarse, que contengan volúmenes de información.

- Manual de formas.
- Manual de procedimientos de los sistemas.

- Descripción genérica.
- Diagramas de entrada, de archivos y de salida.
- Fecha de instalación de los sistemas.
- Proyectos de instalación de nuevos sistemas.

Con base en el desarrollo de este capítulo, podemos agregar que la evolución de las sociedades así como su creciente demanda de información, requieren cada vez más la creación de sistemas tendientes a satisfacer sus necesidades presentes y futuras, dando origen al desarrollo de una variedad de sistemas, tanto manuales como electrónicos, donde cada uno reviste características inherentes a su estructura, mismas que proporcionan ventajas y desventajas, dependiendo del tiempo y lugar donde sean aplicados. Por lo tanto, la decisión de cual de ellos adoptar, está en relación directa a las necesidades a satisfacer, considerando que la tecnología está en constante avance.

CAPITULO II

FUNCIONES DEL AREA DE AUDITORIA INFORMATICA

El mundo de hoy, inmerso en una revolución tecnológica que está impactando prácticamente todas las actividades humanas. Los avances de la informática y las telecomunicaciones han propiciado cambios en los modos de operación y en la estructura interna de todo tipo de organizaciones. Esto ha dificultado la agrupación de las funciones orientadas a precisar las actividades de auditoría informática.

Los autores que tratan el tema tienen diferentes puntos de vista:

- Mair describe las funciones de un centro de proceso en: aplicaciones, desarrollo de sistemas y proceso de datos; y propone que la auditoría informática sea la auditoría de éstas, proponiendo tácitamente la misma agrupación de funciones.[1]

- Lazcano y Rivas se refieren a la auditoría en informática y proponen el enfoque de auditoría sin la computadora, auditoría con la computadora, auditoría a la gestión informática y auditoría funcional a los sistemas de información computarizados.[2]

- Davis lo enfoca desde el punto de vista de los controles de entrada, de salida, sobre el procesamiento y sobre la protección de registros y archivos.[3]

- Weber lo analiza como control en la gerencia y control en las aplicaciones.[4]

---

1 Vid. Mair, William C.; Wood, Donald R., et. al., Computer Control & Audit, p.254

2 Vid. Lazcano, Juan Manuel y Rivas Zyvy Enrique, Auditoría en Informática, Estructuras en Evolución, pp.111-112

3 Vid. Davis, Gordon, B., La Auditoría y el Proceso Electrónico de Información, p.192

4 Vid. Weber, Ron, EDP Auditing, Conceptual Foundations and Practice, p.890

Como podrá observase, pocas son las similitudes, y tal vez haya tantos enfoques como autores, sin embargo, se debe considerar que la agrupación tiene como objeto el dar claridad a las actividades que se desarrollan en auditoría de sistemas, y en este caso en particular, el propósito es presentar una agrupación que sea la base para proponer las áreas que deben integrar la auditoría informática.

En este sentido, y tomando en consideración las diferencias entre los conocimientos y procedimientos que se requieren para auditar las actividades de administración de informática, de desarrollo y de operación de sistemas, así como la necesidad de apoyar la ejecución de auditorías tradicionales con técnicas de automatización de procedimientos, en la presente investigación, propondremos que la auditoría informática sea dividida en tres grandes funciones:

- Auditoría a la Gestión Informática
- Auditoría a los Sistemas en Desarrollo
- Auditoría a los Sistemas en Operación

Es importante aclarar, con el objeto de no ser repetitivos, que los tres grupos son funciones independientes; de apoyo a la actividad ejecutada por los órganos directivos; orientados básicamente hacia el estado operativo pasado, presente y futuro del área informática, del software y del hardware utilizado o a utilizar; que deben tener un total acceso, cuidando los casos de información confidencial, a los documentos, manuales del usuario, de operación o del sistema, y al personal responsable directamente de cualquier actividad, sistema, programa, archivo, etc, sujeto a revisión; las cuales se desarrollaran con estricto apego a las normas y principios generales de auditoría, los principios de la administración, la normatividad del organismo en cuanto a planes, programas, presupuestos, etc.

Es conveniente señalar que frecuentemente se confunden las funciones de auditoría informática y las de apoyo informático, por lo tanto, es recomendable que quede clara la diferencia de la auditoría informática, para evitar que el personal que se asigne a este tipo de actividad en áreas de controlaría interna sea llamado a resolver problemas de la competencia del apoyo informático, por lo que es necesario considerarla como una función mas, independiente del área de auditoría informática, dado que su enfoque es diferente.

2.1 Auditoría de la Gestión Informática

La auditoría a la gestión informática se orienta básicamente a la verificación, examen y valuación de la administración y control de las operaciones en las áreas informáticas o en los centros de cómputo; asimismo, a la economía, eficiencia y eficacia con que se están alcanzando las metas y objetivos, vigilando además que el manejo y aplicación de los recursos asignados (humanos, técnicos, financieros y de información), responda a las políticas, objetivos y proyectos vigentes en la organización.

Cabe destacar, según el modelo conceptual propuesto por Reddin[5] la diferencia entre administración eficiente y administración eficaz, a saber:

Administración eficiente	Administración eficaz
- Hace las cosas de manera correcta - Resuelve problemas - Cuida de los recursos - Cumple con su deber - Reduce costos	- Hace las cosas correctas - Produce alternativas creativas - Optimiza la utilización de los recursos - Obtiene resultados - Aumenta las ganancias

Por otra parte, la mayoría de las operaciones y sistemas de administración y control son procedimientos que se encuentran relacionados a la utilización, optimización y mantenimiento de los recursos del centro de cómputo, incluyendo la adquisición y/o desarrollo de los recursos y su modificación, así como la utilización de servicios de procesamiento externo.

En forma general, los objetivos de la auditoría a la gestión informática son: comprobar con un alto grado de acierto si todos los procedimientos establecidos logran fluidez, consistencia y oportunidad en la administración informática; encontrar los puntos críticos que la entorpecen y promover soluciones rápidas, además de hacer críticas estrictas de tales procedimientos y confirmar si esa es la mejor forma de hacerlo o es factible optimizarlos. En otras palabras, revisar y dictaminar sobre cualquier irregularidad dentro de la organización que atente contra la seguridad del personal e instalaciones, exactitud y totalidad de los datos, procesos y reportes generados para la función de procesamiento de datos.

---

[5] Chiavenato, Adalberto, Introducción a la Teoría General de la Administración Pública, pp. 441

Específicamente, los principales objetivos que persigue la auditoría a la gestión informática, en apoyo a la función directiva, son los siguientes:

- Revisar y evaluar la planeación estratégica de sistemas, con el fin de determinar su congruencia con las metas y objetivos de la organización.

- Revisar y evaluar los sistemas de operación, registro, control e información, con el fin de determinar si funcionan adecuadamente en los términos de las disposiciones aplicables; si contribuyen a alcanzar las metas y objetivos previstos, así como proponer recomendaciones que propicien el mejor desarrollo de las actividades auditadas.

- Evaluar la economía, eficiencia y eficacia con que se logran las metas en relación con los presupuestos asignados (para que pueda medirse la eficiencia y eficacia, es necesario que los recursos empleados, las metas y los logros alcanzados, se expresen en términos cuantitativos).

- Asegurar el establecimiento de criterios que respondan principalmente a :

  - La racionalidad en la obtención y manejo de los recursos en términos de calidad, cantidad, oportunidad, utilidad y precio.

  - El aprovechamiento pleno de la realización de esfuerzos evitando duplicidades o tareas innecesarias.

  - Garantizar que la cantidad de personal asignado a las labores sea suficiente y en ningún caso excesiva que propicie prácticas ociosas.

El alcance de la auditoría a la gestión informática lo comprenden las operaciones o funciones del área informática.

A la auditoría a la gestión informática le competo verificar si los centros de cómputo, están logrando los propósitos para los que se aprobaron los programas y se asignaron los presupuestos, y si tales objetivos o propósitos se alcanzan en forma económica, eficaz y eficiente.

Consecuentemente, el ámbito de actuación de la auditoría a la gestión informática, abarca todas las áreas, operaciones, sistemas, programas, recursos y actividades que integran la gestión informática. Las principales funciones u operaciones de la gestión del área informática sujetas a revisión, se pueden catalogar como sigue:

1. Planear para la organización y para los sistemas de información
2. Establecer políticas, estándares y procedimientos
3. Establecer responsabilidades organizacionales y de administración de personal
4. Controlar la calidad de los sistemas de información
5. Prever requerimientos de servicios externos
6. Establecer la metodología del ciclo de vida del desarrollo de sistemas
7. Establecer los estándares, características o requisitos de software y hardware para el desarrollo y operación de los sistemas
8. Establecer los controles de acceso y seguridad física
9. Prever la salvaguarda y recuperación de los sistemas y de la información.
10. Administrar los servicios auxiliares para la correcta operación de la infraestructura informática (aire acondicionado, sistemas de energía ininterrumpida, mantenimiento a los equipos, limpieza en general, etc.)
11. Establecer planes de contingencia

Revisión de Controles Específicos.-

La auditoría de los controles específicos en un sistema de información, también llamados controles de aplicación, abarca:

- El ciclo de vida del desarrollo de un sistema de información en particular.
- La auditoría de sistemas de información en operación.

En esta área de participación, la preocupación fundamental es la revisión de los controles que garanticen el adecuado acceso, confiabilidad, utilidad y oportunidad de la información cuando el sistema está en operación normal.

Revisión de Controles Generales.-

La auditoría de los controles generales abarca la revisión de todos aquellos aspectos cuyas debilidades no afectan a una información específica, sino en general a cualquier recurso informático.

Los aspectos que abarca la revisión son:

- **Administración de la Función Informática**

Como en cualquier auditoría administrativa, el propósito es verificar que los objetivos de la función se cubran satisfactoriamente y estén de acuerdo con los objetivos de toda la organización. En particular en la función de informática, la auditoría administrativa debe garantizar que los recursos: información, energía, dinero, equipo, personal y materiales son adecuadamente coordinados por la dirección.

- **Adquisiciones de Bienes Informáticos**

Una de las áreas de auditoría más conflictivas y sensibles en una organización es la función de adquisiciones que, tratándose de bienes informáticos se torna aún más sensible, por las dificultades materiales y de evaluación de los mismos.

Los objetivos particulares de esta revisión, englobados en los correspondientes al área de informática son los siguientes:

- Economía y factibilidad del proyecto de inversión para la solución a la problemática planteada en la organización, evaluando su efectividad de acuerdo al objetivo pretendido.
- Protección contractual adecuada, por las cláusulas del contrato que señalan las obligaciones del proveedor y su límite de responsabilidad. Este objetivo toma una capital importancia por los activos involucrados en este ambiente.
- Adaptaciones y/o modificaciones mínimas. Esto se aplica particularmente para la compra de software.

El proceso de evaluación de esta actividad abarca los conceptos de equipo (hardware) y programas (software).

- **Seguridad Física y Lógica**

La seguridad física, se refiere a las medidas físicas que garanticen satisfactoriamente la continuidad del servicio: construcción de las instalaciones, medidas en relación al fuego, humedad, acceso físico a equipos, programas y datos, planes de contingencia, etc.

La seguridad lógica, se refiere al mecanismo del control que garantice que el acceso a los recursos (hardware, software y datos) esté restringido al personal autorizado de acuerdo al nivel jerárquico y funciones del personal.

- **Sistemas Operativos**

La auditoría al sistema operativo consiste en verificar que existan y se cumplan los controles sobre la implantación (opciones elegidas) y controles sobre las modificaciones o nuevas versiones de actualización al mismo.

2.2 Auditoría a los Sistemas en Desarrollo

La auditoría a los sistemas en desarrollo se orienta básicamente a la verificación, examen y evaluación de las etapas del desarrollo de sistemas, específicamente lo referente a la identificación de requerimientos o solicitud de los usuarios, análisis, diseño, construcción, prueba, implantación y liberación del sistema, con el propósito de garantizar un adecuado grado de economía, eficiencia y eficacia en el logro de las metas y objetivos de cada una de las etapas del desarrollo y del sistema mismo; vigilando además que el manejo y aplicación de los recursos asignados (humanos, técnicos, financieros e información), responda a las políticas y objetivos del proyecto o sistema y de la organización.

La auditoría a los sistemas en desarrollo requiere de una ardua labor en múltiples áreas de conocimiento, convirtiendo a los analistas en técnicos multidisciplinarios, exigiendo de ellos una gran dedicación: creatividad (junto con el usuario), que se verá plasmada en el diseño del sistema; un alto grado de conocimiento del área a la que va enfocado el sistema (ejemplo: si se manejan impuestos, deberá tener un amplio dominio del manejo de los conocimientos fiscales, tributarios, etc.; si se utilizan cuentas por cobrar, deberá conocer los principales aspectos contables que se involucran con ese rubro, etc.); así como el conocimiento y experiencia de las principales técnicas de programación más recientes o importantes en el medio de la informática; lo cual propicia dos beneficios concretos:

1. Contar con alguien capacitado para esta labor

2. Incrementar la independencia del auditor debido a su capacidad técnica

En forma general, los objetivos de la auditoría a los sistemas en desarrollo son: garantizar el óptimo y adecuado desarrollo del sistema en atención a la normatividad, políticas y necesidades del área o departamento solicitante.

Los objetivos particulares que persigue esta area de participación del auditor en informática son los siguientes:

- Prevenir la omisión de controles adecuados y verificar la suficiencia de los mismos, incorporados a lo largo del desarrollo del sistema.

- Revisar y evaluar los sistemas con el fin de determinar si se están desarrollando adecuadamente, de acuerdo con las especificaciones del proyecto, la normatividad y los lineamentos establecidos al respecto; y, si contribuyen a alcanzar las metas y objetivos previstos, así como proponer recomendaciones que propicien el mejor desarrollo de las aplicaciones o programas auditados.

- Validar la oportunidad y costo-beneficio del desarrollo o modificación del sistema.

- Monitorear el avance en el desarrollo del sistema.

- Verificar que el sistema sea comprensible, tanto para técnicos, usuarios y terceras personas.

- Lograr que el sistema sea auditable, incorporando controles necesarios para poder rastrear una aplicación o transacción durante el flujo normal de la operación.

- Verificar que los sistemas se encuentren totalmente documentados por medio de la elaboración de manuales técnicos y del usuario.

- Garantizar la implementación de los mecanismos de control necesarios para el adecuado funcionamiento del sistema y salvaguarda de la información (restricción en el acceso, validaciones, privilegios, etc.)

El alcance de la auditoría a los sistemas en desarrollo, dependerá de la importancia de los programas, aplicaciones, reportes y datos del sistema dentro del proceso electrónico de datos.

"Cuando el auditor participa en todo el proceso de desarrollo de sistemas, los objetivos son asegurar que el sistema esté desarrollado sobre una estructura de control adecuada y suficiente para salvaguardar los activos, asegurar la integridad de los datos y lograr sistemas eficientes y efectivos."[6]

En general, las principales funciones u operaciones de la auditoría a los sistemas en desarrollo se pueden catalogar como sigue:

1. Por función o sistema
2. Por tipo de equipo
3. Por usuario

En un plano mucho más amplio, se identifican diversas áreas o actividades sujetas a revisión con la finalidad de limitar el universo, es decir, especificar los alcances que tendrá la auditoría, por ejemplo:

- Diseñar y establecer los modelos funcionales y modelos de datos
- Establecer los diagramas entidad-relación
- Definir los diccionarios de datos
- Establecer el modelo de distribución de datos

---

[6] Weber, Ron, op. cit., p.107

- Prever servicios externos de desarrollo de sistemas
- Realizar las actividades del ciclo de vida del desarrollo de sistemas de acuerdo a la metodología y estándares
- Realizar y documentar fase de iniciación de proyecto
- Realizar y documentar fase de estudio de factibilidad
- Realizar y documentar fase de diseño del sistema
- Realizar y documentar fases de desarrollo e implantación
- Realizar y documentar fase de mantenimiento
- Realizar fase de post-implantación

Uno de los principales controles sobre el desarrollo de sistemas de aplicación, es que el auditor forme parte del equipo de desarrollo. "Aún cuando el auditor esté interesado en todos los aspectos del nuevo sistema - control, eficiencia, información gerencial, seguridad, etc. -, su mayor interés estará en sugerir y evaluar los controles de aplicación. Consecuentemente, su principal contribución es asegurar que las aplicaciones automatizadas, recientemente implantadas, incluyan características de control sólidas y confiables."[7]

El hecho que el auditor participe en el desarrollo de nuevos sistemas, no elimina la necesidad de un examen de los sistemas de aplicación existentes. Lo que hace, en términos generales, es prevenir que se implanten sistemas de aplicación que tengan riesgos importantes.

El auditor interviene revisando y aprobando la documentación generada como producto final de las actividades. Esto no quiere decir que el auditor autorice la continuación del proceso de desarrollo, o que proporcione una garantía absoluta de que no se ha omitido ningún control; sino simplemente, que debe tomar una decisión con respecto a si los productos finales de la documentación son o no adecuados.

---

[7] Mair, William C.; Wood, Donald R., et. al., op. cit., p.341

Un aspecto más que obliga a la participación del auditor en los sistemas en desarrollo, es la poca participación, tanto de los directivos como de los usuarios, dando origen a los sistemas que prácticamente son controlados por el personal del área de sistemas. Una participación idónea dará como resultado sistemas equilibrados, que respondan integralmente a las expectativas de la dirección y a las necesidades de los usuarios, con la ayuda óptima del área de sistemas y con la tecnología disponible.

Al mismo tiempo, el auditor debe seguir siendo independiente, estar consciente de que su revisión tiene limitaciones y continuar informando sobre cualquier riesgo importante que detecte.

En las organizaciones grandes y medianas, la comunicación se convierte en un problema significativo, por lo que desde un inicio deberán existir estrechos vínculos entre la dirección, los auditores, el área de sistemas y los usuarios, siendo de suma importancia el dejar constancia clara y por escrito de las decisiones tomadas a lo largo del ciclo de vida del sistema, con objeto de lograr un mayor entendimiento.

De este modo, la documentación garantizará una continuidad en el proceso que asegure la realización del objetivo de las partes involucradas, cuando el sistema se convierta en una realidad operativa.

El área de sistemas debe contar con un patrón formal o metodología, es decir, con un conjunto de procedimiento sistemáticos que permitan la estandarización en el proceso y eviten deficiencias, inexactitudes e inconsistencias.

2.3 Auditoría a los Sistemas en Operación

La auditoría a los sistemas en operación se orienta básicamente a la verificación, examen y evaluación del funcionamiento de los sistemas que están siendo utilizados, con el propósito de garantizar el logro de las metas y objetivos de éstos, con un adecuado grado de economía, eficiencia y eficacia, vigilando además que el manejo y aplicación de los recursos asignados (humanos, técnicos, financieros e información), responda a las políticas y objetivos del sistema y de la organización.

Los objetivos de la auditoría a los sistemas en operación son: obtener resultados en forma consistente y oportuna del procesamiento de datos; identificar los puntos críticos que entorpecen su funcionamiento y promover soluciones rápidas a éstos en forma óptima y adecuada.

Específicamente, los principales objetivos que persigue la auditoría a los sistemas en operación, en apoyo a la función directiva, son los siguientes:

- Asegurar que toda la información fue procesada en forma correcta y oportuna, y que de dicho proceso se obtuvo la información esperada.
- Evaluar la utilización de recursos y dar una opinión respecto a la economía, eficiencia y eficacia con que se emplean.
- Monitorear la operación del sistema.
- Garantizar la alimentación confiable de datos al sistema en forma oportuna y confidencial.
- Asegurar que los reportes lleguen a su destino final sin pérdidas o fugas de información en el trayecto de la máquina al usuario final.
- Asegurar la destrucción total de formas preimpresas (cheques, recibos de pagos, etc.) mal impresas o desperdiciadas, etc.
- Verificar si el sistema sigue siendo útil al usuario.

El alcance de la auditoría a los sistemas en operación, dependerá de la importancia de los programas, aplicaciones, reportes y archivos del sistema dentro del proceso electrónico de datos.

A la auditoría a los sistemas en operación le compete verificar el desenvolvimiento o funcionamiento de los sistemas de cómputo de la organización, si se están logrando los propósitos para los cuales fueron desarrollados y si tales objetivos o propósitos se están alcanzando en forma económica, eficaz y eficiente.

De esta manera, el ámbito de actuación de la auditoría a los sistemas en operación abarca todas las áreas, operaciones, subsistemas, programas, recursos y actividades involucradas en la operación de un sistema determinado.

En general, las principales funciones de la auditoría a los sistemas en operación se pueden catalogar como sigue:

1. Por dispositivos de los equipos de computación, red, periféricos magnéticos, impresoras, controladores, etc.
2. Por sistemas
3. Por usuarios
4. Por los resultados generados

En un plano mucho más amplio, se identifican diversas áreas o actividades susceptibles de revisión, con la finalidad de limitar el universo, es decir, especificar los alcances que tendrá la auditoría, como ejemplo de éstas se mencionan las siguientes:

- Preparar información
- Capturar información
- Transmitir información
- Procesar información
- Resguardar y restaurar información
- Emitir reportes y/o archivos
- Seguridad lógica
- Controlar el acceso y seguridad física
- Distribuir reportes
- Controlar los cambios de versión a los sistemas en operación
- Administrar los recursos de los equipos de cómputo (área en disco, memoria, privilegios de usuarios, etc.)
- Monitorear las operaciones de procesamiento distribuido y redes
- Administrar los suministros (discos, cintas, papelería, formas preimpresas, etc.)

De acuerdo con lo expuesto en este capítulo podemos concluir que la creciente implantación de sistemas de cómputo en las organizaciones, hardware y software más sofisticados, así como los grandes volúmenes de información que se manejan, han originado la necesidad de crear una metodología de control y evaluación que permita prever su adecuada utilización.

Dada la importancia en la veracidad de la información generada, es necesario contar con los procedimientos y controles apropiados para que los sistemas de información computarizados mantengan el nivel de confiabilidad y eficiencia, y cumplan con los objetivos de las organizaciones. Ante tal hecho, es notoria la necesidad de aplicar la auditoría al campo de la informática, haciendo uso de nuevas técnicas y herramientas.

CAPITULO III

METODOLOGIA PROPUESTA PARA REALIZAR UNA AUDITORIA INFORMATICA

3.1 Preparación de una Auditoría Informática

Antes de implantar un programa general de auditoría informática, es indispensable contar con la aprobación y pleno respaldo de la dirección. Al organizar un programa de auditoría de sistemas, es muy importante la existencia de una política que señale objetivos y refleje un plan bien definido para su logro.

Este plan debe incluir la selección de personal adecuado para la realización de la auditoría, determinando las tareas y procedimientos que se seguirán, y el establecimiento de una base de control de tiempo y costo.

Al preparar un plan de metas, es indispensable determinar las necesidades generales y su relación y precisar si éstas abarcan todos los aspectos para el logro del objetivo.

Para estructurar un programa que dé buenos resultados en una organización, se necesita primero definir su alcance, lo cual es básico en la obtención de los resultados. La auditoría informática puede abarcar un sistema en su totalidad, un subsistema o un sector de él, siempre y cuando se cuente con personal calificado y en número suficiente.

No sólo debe existir un acuerdo con la dirección de la empresa, en cuanto a la naturaleza, alcance, detalle y personal, sino también se requiere la determinación de funciones, responsabilidades y fijación de compromisos de los responsables de la auditoría informática, ya sea un grupo especializado o un departamento.

El tiempo y costo de la auditoría informática será diferente en cada trabajo, dependiendo de la naturaleza del sistema, su magnitud, su complejidad y el número de personas destinadas a la auditoría, definiendo si se requiere de la ayuda de consultores o de auditores externos.

Toda auditoría informática inicia en un estudio preliminar, a efecto de precisar de qué se trata, cuánto y qué tipo de personal se necesita y el tiempo que ésta se llevará. Posteriormente, se aplicará una metodología de evaluación para determinar lo adecuado del funcionamiento del sistema, el cumplimiento de políticas y procedimientos, la exactitud y confiabilidad de los controles, los métodos adecuados de protección, las causas de desviaciones, la utilización correcta de los recursos asignados y los métodos satisfactorios de operación.

Esto se lleva a cabo por medio de una recopilación de información (a través de entrevistas, inspecciones, diagramaciones, etc.), posteriormente un análisis, interpretación y síntesis de la información recopilada (estudiando los elementos, realizando un diagnóstico detallado, investigación de las deficiencias, búsqueda de problemas, determinación de alternativas, etc.); se hacen luego pruebas de todos los aspectos de la operación, se analizan cuidadosamente los resultados y por último se prepara el informe final, el que comprenderá los hechos más importantes que se hayan encontrado y las evaluaciones de las operaciones, incluyendo las recomendaciones a las observaciones realizadas, con los medios alternativos para ponerlas en práctica. Asimismo, se programa un conjunto de revisiones posteriores para medir la efectividad de lo que se llevó a cabo.

3.1.1 Necesidad de una Acción Persuasiva

Para que la auditoría informática cumpla con el objetivo de auxiliar a los responsables de sistemas en ejecución, proporcionando información sobre su eficiencia, eficacia, y el logro de objetivos y metas establecidos, el auditor necesita tener habilidad para enfrentar las dificultades que suelen encontrarse. Conviene que el auditor reflexione con cuidado antes de actuar, ya que puede toparse con personas que piensan que nada podrá mejorar sus sistemas, convencidos de que son eficientes en alto grado; o bien, con personas que quieran que se les demuestre que obtendrán beneficios y requieran estudiar a fondo toda clase de sugerencias o recomendaciones.

El tratar con personas y con problemas que involucran el elemento humano, exige paciencia y comprensión. Cuando surgen diferencias de opinión (como a menudo ocurre en las relaciones humanas), se deben tratar con cuidado. Por ejemplo, habrá ocasiones en que el auditor se encuentre con ejecutivos que se opongan a aceptar sugerencias para el mejoramiento de su actuación, principalmente por ser reacios al cambio.

En todos los casos de resistencia, el auditor deberá buscar su verdadera causa, ya que, no toda conducta que se opone al cambio puede juzgarse como resistencia, puede estar motivada por otras causas: tal vez por que la persona no simpatice con quienes busquen el cambio, o por que ella haya sugerido el cambio en otra época y se le haya negado.

Es por ello que el auditor debe ser comprensivo, discutir los principales elementos involucrados en el cambio con los afectados, señalar la necesidad del mismo y dejar muy clara la postura de la dirección en favor de un mejoramiento.

Poco puede hacerse mientras que el responsable de sistemas no tome conciencia de los problemas y de las responsabilidades de mejorar su área y se comprometa a colaborar en la realización de la auditoría. Si esto no se logra, tendrá tendencia a creer que la dirección no esta satisfecha con su trabajo, en consecuencia, tratará de esconder los problemas y puntos deficientes de su organización, argumentando que no es posible reunir la información que requiere el auditor. Buscará justificar las decisiones tomadas y se ocupará de detectar fallas en el auditor de sistemas, neutralizando el efecto que los reportes de auditoría pudieran producir en la dirección.

En último caso, tratará de poner a sus subordinados contra el auditor, haciéndoles creer que las peores consecuencias para ellos resultarán de su intervención en la auditoría (mayores controles, reorganización del área, ajustes de personal, etc.).

3.1.2 Solicitud Oficial de Auditoría

Hay un problema que se presenta con cierta frecuencia en las organizaciones, cuando la dirección no se entera y por lo tanto no llama la atención a los ejecutivos que no cumplen con las políticas establecidas, o cuando realizan cambios en los sistemas y procedimientos, sin avisar debida y oportunamente a las áreas que resultan afectadas.

Muchas veces, se realizan modificaciones a los sistemas sin tener en cuenta las necesidades de otros departamentos, esto suele ocasionar que el auditor se encuentre en un ambiente en donde cada persona tenga un concepto distinto del sistema y que la realidad de su funcionamiento no se pueda conocer fácilmente.

Como ya se especificó anteriormente, los motivos para la realización de una auditoría pueden ser varios, pero si ésta no va acompañada por una solicitud oficial no podrá llevarse a cabo exitosamente. Esta deberá ser en forma escrita, especificando su objetivo y motivo de solicitud, el alcance que requieran de la auditoría y el sistema y/o subsistemas a revisar.

Solicitando oficialmente la auditoría informática, el responsable del sistema correrá menos riesgos frente a sus colaboradores. Es necesario precisar en este caso:

- Que los responsables del sistema tomen parte en la realización de la auditoría;
- Que las proposiciones que resulten de la intervención sean sometidas; y,
- Que el reporte de auditoría sea confidencial y que su difusión se supedite a su iniciativa.

3.1.3 Selección del Auditor

La auditoría informática deberá ser realizada por personal apropiado para llevar a cabo las tareas.

Primeramente, se requiere definir si la empresa puede realizar con sus propios medios parte o la totalidad de la intervención, o si se requiere de consultores especialistas en esta actividad.

Las razones más importantes en favor de una intervención externa son:

1) La competencia: Si la empresa hace realizar la auditoría a los empleados en el área de sistemas, éstos difícilmente podrán hacer valer nuevas formas de operación por que no las conocen. El auditor externo, por el contrario, tiene una experiencia diversificada que le permite, por comparación con otras situaciones encontradas, detectar rápidamente los puntos débiles de la organización del área de sistemas y proponer soluciones innovadoras.

2) La objetividad de juicio: Los responsables de los sistemas en la empresa y sus subordinados están directamente involucrados en los métodos y procedimientos utilizados en cada sistema, por lo cual, tendrán tendencia a pensar que las cosas son difícilmente mejorables y se inclinarán a la justificación.

Un auditor en sistemas, siendo totalmente ajeno a la empresa, es más objetivo y analizará sin prejuicios la organización del servicio, las aplicaciones informáticas, etc.

En caso de que la empresa forme parte de un grupo industrial, comercial, bancario, gubernamental, puede existir la posibilidad que el mismo personal de sistemas lleve a cabo la auditoría, ya que seguramente dispone de una área central de auditoría, por el tipo de empresa.

El responsable de sistemas, mediante el apoyo de una metodología adecuada, puede proceder a un primer análisis que le permita definir los principales problemas y después recurrir a un auditor externo para resolverlos.

Por ultimo, suponiendo que la necesidad haya surgido por el responsable de sistemas, a éste le corresponde determinar las tareas de las que él se ocupará directamente y cuáles deberán ser realizadas por el auditor externo, en base al grado de técnica de las mismas o de las intervenciones humanas.

En el caso en el que la auditoría informática requiera hacerse por auditores externos, después de un concurso y análisis de las condiciones de intervención (costo, duración, calificaciones, etc.), la dirección y los responsables de sistemas harán la elección del despacho que más le convenga. Uno de los elementos más importantes que intervendrán en la selección, son los factores de los cuales dispone el despacho, como normas, estándares, etc., respaldados por varias intervenciones.

3.1.4 Firma del Contrato

En el contrato se enunciarán los costos, las modalidades de facturación y la duración de la auditoría. Desconociendo el grado de complejidad del sistema o sistemas a auditar y la importancia de los problemas a detectar, la fórmula que se propone en esta metodología es la *intervención por hora*.

En la práctica, la fórmula que más se utiliza es la de un ajuste a destajo para una duración de algunas semanas, cuyo costo no represente un porcentaje superior al 2% del presupuesto de los sistemas de información.

Al considerar los costos de auditoría, conviene incluir el tiempo que utilizarán los responsables de sistemas, así como también las intervenciones de los usuarios.

Se recomienda que la intervención de auditoría de sistemas no se prolongue demasiado porque perdería impacto, las sugerencias posiblemente no serían las adecuadas y no tendrían límites las mejoras y los problemas de estudio.

Definir a priori la duración de la auditoría es quizá la mejor solución, por que obliga al auditor de sistemas a detectar rápidamente los problemas principales.

Una vez que se hayan definido todos estos elementos, podrá firmarse el contrato.

3.1.5 Programa de Auditoría Informática

Antes de iniciar la auditoría informática, recomendamos reflexionar con calma para establecer un programa de actividades, que consistirá en una serie de factores a revisar y los métodos y procedimientos a seguir, encaminados a los objetivos de cualquier auditoría.

Un programa de auditoría informática contendrá los siguientes aspectos:

1.- Establecimiento de los objetivos en la revisión.

2.- Definición de las tareas de la auditoría de sistemas, identificando sus jerarquías.

3.- Planteamiento del desarrollo de las tareas simultáneas y su secuencia, así como las actividades respectivas.

4.- Programación del trabajo de acuerdo con los requerimientos de la dirección; estableciendo las fechas de terminación y restricción de actividades.

5.- Estimación de costos de la auditoría.

La evaluación de un sistema deberá comprender tres aspectos básicos que son:

- La satisfacción en su totalidad de las necesidades de las áreas involucradas;
- El funcionamiento eficaz del sistema en la organización; y,
- El grado de eficiencia y los resultados obtenidos a través del sistema.

La auditoría informática debe planearse de tal manera que se ajuste a cada una de las situaciones individuales de cada sistema, pero siempre bajo una metodología básica.

3.1.6 Métodos de Auditoría Informática

3.6.1.1 Auditoría sin Auxilio de la Computadora

Consistirá en la evaluación del control interno, incluyendo la revisión del sistema para comprobar cómo debe trabajar y qué controles debieran estar en operación, y pruebas del sistema para acumular evidencia acerca de cómo funciona en la realidad. Asimismo, se evaluarán los informes preparados por la computadora.

La revisión del sistema se deberá llevar a cabo por medio de entrevistas con personal del sistema, uso de cuestionarios, exámenes de descripción del sistema, revisión general de los principales controles, etc.

Las pruebas del sistema se llevarán a cabo a través de:

- Examen de la evidencia de controles (listados de errores, registros de control, autorizaciones, etc.).

- Uso de listados para comprobar partidas desde los datos de entrada hasta los documentos de origen, informes y controles.

- Comprobación de una operación de muestra respecto a su correcto procesamiento y la ejecución de otras pruebas que sean necesarias en cada caso.

Esta metodología de revisión, se orienta a la aplicación de procedimientos tradicionales de auditoría para verificar manualmente el comportamiento y validez de las transacciones ocurridas y registradas, y en los casos en que se cuente con sistemas de información automáticos, estos procedimientos pierden efectividad, lo que es complicado cuando se tiene, ya que sólo se pueden aplicar procedimientos de revisión externos al procesamiento electrónico de datos.

Entre las principales limitaciones que se tienen con esta metodología, destaca el hecho de que generalmente sólo se puede disponer en forma reducida de registros impresos, haciendo caso omiso de todos aquellos registros magnéticos que carecen de representación visual.

En este enfoque, sólo se puede determinar desde un nivel primario, la confiabilidad de las entradas y de los resultados obtenidos, sin poder determinar la validez de su procesamiento.

La aplicación de técnicas de muestreo estadístico ha venido a auxiliar en la selección de partidas susceptibles de verificación; sin embargo, no deja de ser éste un primer plano de revisiones que de ninguna manera permite lograr su plena interpretación y análisis.

Los factores para seleccionar este tipo de auditoría en un sistema son:

- Que se trate de un sistema de salida completo y en donde existan claras referencias cruzadas que puedan asociarse fácilmente a los conceptos de los datos fuente, de los cuales se derivaron dichas salidas.

- La existencia de cantidades significativas de actividades de procesamiento manual en el sistema completo.

- Un número limitado de transacciones para cuyo manejo a sido diseñado el sistema.

- Un volumen pequeño de actividad de procesamiento.

- Un rastreo visible y definido de auditoría a través de todo el sistema.

- Pocos cambios en el programa del sistema.

- La falta de auditores capaces de analizar los procedimientos del sistema o de utilizar el equipo de procesamiento de datos y sus capacidades con fines de auditoría.

Por lo anteriormente mencionado y haciendo una correlación de lo que este tipo de intervención representa en el proceso de las etapas de evolución de la auditoría interna, podemos concluir que cuando el auditor orienta su intervención bajo este enfoque, particularmente en organizaciones que cuentan con sistemas de información computarizados, se está haciendo uso de herramientas que corresponden a una etapa de inicio con las limitantes implícitas en el resultado profesional de su trabajo.

3.1.6.2 Auditoría a través de la Computadora

Las herramientas que principalmente utiliza el auditor, son la configuración del equipo (hardware y software) y los archivos magnéticos de la instalación.

Esta metodología de intervención, persigue fundamentalmente automatizar procedimientos tradicionales de auditoría con fines de evaluación, verificación, análisis e interpretación de la información auditada, que por su aplicación pueden orientarse indistintamente a intervenciones de tipo financiero u operacional.

Cabe destacar que el cuidado y esmero con que el auditor maneje los sistemas informáticos, debe corresponder con el valor que su utilización tiene, ya que en este tipo de trabajo las consecuencias a que el propio auditor puede dar lugar por la comisión de errores, son de mayor impacto y repercusión que en los procedimientos manuales; por citar un ejemplo, diremos que cuando el auditor se equivoca en la elaboración de registros manuales con sólo borrar o tachar enmienda al error, pero cuando la equivocación está en el uso y asignación de archivos magnéticos y de ello logra una integración de datos improcedente o destruye un archivo sin respaldo, las afectaciones a que da lugar son drásticamente más serias.

Entre los principales beneficios que genera el uso de la computadora, destacan el incremento sustancial en los alcances, oportunidad y confiabilidad de la información que se maneja, lo que lleva al auditor usuario de un plano de revisor y certificador de registros manuales, a un plano interpretativo y de análisis del comportamiento de los datos, permitiendo así un mayor nivel de eficacia en sus resultados y en los servicios que proporciona.

En el proceso de utilización de la computadora, inicialmente el auditor orienta sus revisiones con la explotación de información hacia aspectos predefinidos, tales como aplicación de confirmaciones, análisis de vencimientos, muestreo estadístico, etc., que no es más que darle velocidad y volumen a pruebas tradicionales de auditoría previamente especificadas.

En la medida en que se le da mayor utilización a la computadora en la explotación de información, el auditor puede incorporar en forma recurrente, procedimientos automatizados de revisión dentro del ciclo de las auditorías y para ello adecua periódicamente los conceptos predefinidos. Para la aplicación de estos procedimientos automatizados predefinidos, el auditor puede emplear el software denominado "paquetes de auditoría", los que permiten apoyar sustancialmente pruebas típicas y modulares de auditoría.

Cabe subrayar que los paquetes de auditoría no son una solución, sino sólo una herramienta, cuyos beneficios dependen de su utilización.

En una etapa avanzada del uso de la computadora, el auditor define procesos en formato libre (no predefinidos) que eventualmente le requieren de una mayor codificación de registros y de lógica, y en los que utiliza herramientas de usuario final tales como sistemas de consulta en línea, reporteadores o superlenguajes, así como también software de cuarta generación, etc.

Como fruto de la utilización de estos recursos, el auditor llega a diseñar y obtener información en forma permanente a través de sus propios sistemas, que a semejanza de un tablero de control o de un sistema de radar, sistemáticamente le permiten monitorear e identificar desviaciones sobre el comportamiento regular de las transacciones, donde las inconsistencias en términos generales son originadas por errores en el manejo y/o procesos operativos y funcionales.

Entre los principales motivos por los que se requiere la computarización de procedimientos de auditoría, se pueden citar los siguientes:

- Incremento sustancial en los volúmenes de información y alcances de las intervenciones lo que requiere mayor y mejor selección, verificación y análisis de la información.

- Necesidad de mayor oportunidad y profundidad en la revisión, así como del tiempo requerido para la entrega de los resultados de auditoría.

- Importancia de lograr la mayor confiabilidad a través de la precisión y exactitud de la información utilizada (por la eliminación de pasos de operación de datos).

- Posibilidad de un mejor aprovechamiento y utilización de la fuerza de trabajo del personal de auditoría, por la eliminación de labores manuales de obtención de datos y por el incremento en las tareas interpretativas, analíticas y de diagnóstico.

- Necesidad de mantener la independencia operativa y de juicio que se requiere en el análisis y la verificación de la información sin distracción del personal de informática; ya que de otra manera, estaría supeditado a la disponibilidad de este personal para integrar sus elementos de revisión.

Para llegar a la computarización de procedimientos de auditoría, existen diversas opciones donde cada una de ellas tiene sus propios beneficios y restricciones. De acuerdo a los propósitos de nuestra investigación, sólo mencionaremos de manera enunciativa las siguientes opciones: "Adquisición de un Paquete de Auditoría", "Capacitación de Auditores en Informática", y "Contratación de Personal con Experiencia en Informática", donde cada una de ellas es particular y específica.

Respecto a los beneficios que estas distintas opciones persiguen, están el satisfacer algunos de los requerimientos que demandan la computarización de procedimientos. Por otra lado, las restricciones que en términos generales hemos apreciado en las distintas opciones, tienen un grado diferente de impacto según sus características.

En este marco de referencia, en algunas ocasiones se escuchan cuestionamientos y razones acerca de si es mejor "contratar programadores para auditoría" o "capacitar auditores en programación". A este respecto mencionaremos que no sólo es elegir una alternativa, sino también identificar cómo se integra dependiendo del momento en que se encuentra la función de auditoría, así como la estructura de la organización y sus principales requerimientos, ya que de otra manera sólo se busca una respuesta simple (no sencilla), a necesidades de mediana o gran complejidad y esto generalmente no resulta.

Refiriéndonos específicamente a los antecedentes de la comercialización y aplicación de los paquetes de auditoría, podemos mencionar que hacia fines de la década de los '60s, las firmas americanas más grandes de contadores y auditores iniciaron el desarrollo de rutinas preprogramadas para facilitar los trabajos de auditoría dado el creciente volumen de transacciones, ya que para entonces se observa una tendencia en la reducción de los alcances de intercención y en el incremento de los recursos humanos dedicados, tal como se ejemplifica en el siguiente esquema[1].

AÑOS	ALCANCE DE LA INTERVENCION	EQUIPO DE AUDITORIA
1965	49%	4 personas
1967	43%	5 personas
1969	37%	7 personas
1971	31%	10 personas
1973	25%	14 personas

[1] Colegio de Contadores Públicos de México, Diferentes Enfoques de Auditoría en Informática, p.37

Como se observa en este juego de tendencias, aunque los datos presentados son para ejemplificar la inversión, tiene un amplio sentido realista y se debe a que cada día son más las aplicaciones que se automatizan y también es mayor el cúmulo de transacciones que bajo estos mecanismos se procesan.

En la primera mitad de la década de los '70s, la industria del software avizoró la posibilidad de hacer negocio con la integración preprogramada y comercialización de paquetes de auditoría, apoyándose básicamente en sistemas reporteadores o en generadores de programas, para dar satisfacción a un mercado que se veía promisorio. Esto llevó a diversos fabricantes a proyectar productos de alta calidad técnica aprovechando la experiencia de los productos inicialmente desarrollados por los despachos de contadores públicos.

En la actualidad ha proliferado el desarrollo y comercialización de paquetes de auditoría, siendo éstos producidos fundamentalmente por empresas norteamericanas con el propósito de satisfacer necesidades sobre marcas específicas de computadoras en sus distintos tamaños, aunque principalmente para las de gran tamaño o macros.

Aún cuando el propósito de los paquetes de auditoría y de las herramientas de usuario final, es reemplazar las actividades manuales para manejo de datos por procedimientos automatizados, hoy en día no se aprovechan en varias organizaciones, por lo que el tiempo consumido por el auditor para el manejo de datos, oscila entre el 40 y el 70% del tiempo útil.

La celeridad del crecimiento en los sistemas de información y las velocidades del procesamiento electrónico de datos que fluctúan en niveles de 5 a 12 millones de instrucciones por segundo, van marcando una clara desventaja y falta de competitividad en el empleo de técnicas manuales para el manejo de datos contra medios automatizados.

La función de la computadora puede ser una herramienta muy poderosa para la auditoría, y el auditor debe estar actualizado respecto a los avances tecnológicos en el área y sobre las ventajas que obtendría con ello. Asimismo, es conveniente que esté consciente de los problemas que afrontará al usar la computadora.

Ventajas de usar la computadora.- El uso de la computadora por parte del auditor y la revisión del sistema de información proporcionan muchas ventajas:

1. "Un mejor conocimiento del sistema de procedimientos y controles del cliente

2. Un área de actividad mucho más extensa

3. El más fácil logro de la auditoría continua

4. Un mejor uso del principio de excepción."[2]

La auditoría a través de la computadora consistirá en utilizar esta herramienta para obtener información acerca de la operación de los programas y de los controles que tienen incorporados.

Para probar los programas se podrán utilizar dos métodos: mediante datos de pruebas y mediante procesamiento o reprocesamiento controlado.

Método de Datos de Prueba.- Los datos de prueba son un conjunto de operaciones de muestra para ser procesados por el programa de la computadora sometido a prueba. Los pasos generales para preparar y utilizar los datos de prueba son:

- Determinar los tipos de registros maestros que van a ser utilizados.
- Determinar los tipos de operaciones que van a ser incluidas en los datos de prueba.
- Preparar papeles de trabajo adecuados.
- Obtener los registros que van a ser procesados con las operaciones de prueba, determinar previamente los resultados, para compararlos con los datos reales de salida del procesamiento de prueba.
- Si las operaciones de prueba son corridas con los archivos maestros regulares o con la corrida regular del procesamiento, investigar los efectos que el procesamiento de prueba tendrá sobre la información de salida del sistema.
- Obtener los programas que van a ser probados y verificar que los programas son utilizados en el procesamiento de las operaciones de prueba.

---

[2] Vid. Porter, W. Thomas, Jr., Auditoría de Sistemas Electrónicos, p.131

- Hacer arreglos para la preparación de las operaciones de prueba y para la formulación de información de salida en una forma útil.

Para efectos de preparación y revisión de las pruebas, es preciso que queden documentadas en papeles de trabajo, que deberán incluir: control de datos de prueba, información sobre las operaciones y soluciones; información del archivo maestro; matriz de datos de prueba y listado de la computadora.

Método de Procesamiento o Reprocesamiento Controlado.- Es aquel en el que se controla la corrida del procesamiento utilizando un programa que ha sido aprobado.

Cuando se utilice el reprocesamiento para comprobar el proceso de operaciones efectuadas durante el período auditado, se deben obtener copias de los archivos de operación antes de que sean desechados.

El procesamiento o reprocesamiento controlado implica bastante uso de la computadora, tanto para controlar el programa como para controlar su corrida.

Por lo tanto, el método deberá ser utilizado únicamente si el volumen de datos para procesar y comprobar es considerable, o si el procesamiento que se va a verificar es complejo y difícil de seguir por medio de listados visibles.

Los factores que determinan la utilización de la computadora en la auditoría son:

- Que se trate de un sistema con uso extensivo de mantenimiento mecanizado de archivos, en el cual, archivos maestros de cintas magnéticas se actualicen mecánicamente.

- Que la producción de casi todas las salidas normales del sistema sea en una forma resumida, haciendo posible la identificación de conceptos individuales de los datos fuente.

- Que el sistema cuente con diferentes tipos de transacciones acopladas a un volumen relativamente grande de actividades del sistema, de tal manera que el muestreo sea muy difícil o impráctico.

- Que existan cambios frecuentes en el programa de instrucciones de prueba de operación.

- Que la computadora en el sistema sea la parte fundamental del procesamiento de datos.

Por otro lado, los problemas que se presentan para el uso de la computadora en auditoría son:

- Costos
- Requerimientos técnicos
- Necesidad de planear por adelantado
- Conversión

Sin embargo, el proceso de conversión no siempre ocurrirá cuando el trabajo de auditoría esté realizándose. No obstante, la probabilidad de que el auditor se encuentre con una conversión, es considerable. La conversión es un período arduo, laborioso y de mucha presión causada por las exigencias del tiempo y de la gerencia. Debido a estas presiones, es posible que el auditor se enfrente a varias dificultades:

- Falta de documentación significativa
- Sobrecargas de trabajo de los programadores, que dificultan el acceso
- Cambios frecuentes de programa, que dificultan la revisión y evaluación del sistema

3.2 Metodología de la Auditoría Informática

El primer paso es definir el sistema que se va a auditar, las áreas del sistema que requieran una revisión más detallada y profunda y las etapas del sistema que se auditarán.

Los aspectos a revisar principalmente serán:

1. El análisis preliminar. En donde se evaluará la detección de las necesidades para la justificación del proyecto; si se trata de un sistema manual, se estudiarán las causas que originaron el sistema.

2. La planeación del proyecto. Comprende el análisis del estudio de viabilidad, la selección del sistema, la coordinación y control del proyecto y el programa de pre-instalación.

3. El análisis de información. Se revisan las necesidades de información, sus fuentes y la documentación del sistema.

4. La organización del proyecto. Se evalúan los procedimientos, el desarrollo del personal, el tratamiento y el uso de la información.

5. El desarrollo del sistema. Se analiza el cumplimiento de objetivos, la satisfacción de las necesidades, la efectividad del sistema y la ejecución de compromisos y responsabilidades.

3.2.1 Enfoque y Alcance de la Auditoría

En esta fase se especificará cual será el enfoque que se le de a la auditoría, ya sea solo una revisión superficial o una especifica, a una sola etapa del sistema o el análisis completo del mismo.

Los indicadores para establecer el enfoque y alcance de la auditoría estarán implícitos en la solicitud de la misma, siendo determinados por las causas que originan esta revisión. Entre ellas, puede mencionarse el mal funcionamiento en una parte del sistema, el retraso de información, los reportes incompletos, los controles inadecuados, etc. Dependiendo de la problemática existente en el sistema que se auditará será el enfoque y alcance de esta misma.

Otro aspecto muy importante de tomarse en cuenta es el tiempo que se ocupará en la auditoría. Para determinar el tiempo estimado requerido se deben considerar tres elementos: primero, la magnitud de los problemas a estudiar; segundo, la amplitud que se le va a dar al estudio de acuerdo con los resultados que se pretende obtener, además del personal que se tenga disponible; y, como tercer elemento, la experiencia obtenida en revisiones anteriores en cuanto a la participación y facilidades que brinde el personal del sistema.

3.2.2 Preparación del Programa de Auditoría Informática

Antes de iniciar la auditoría informática, se requiere de un programa de actividades, en el cual se encontrarán los factores a revisar, los métodos y procedimientos a seguir y el tiempo aproximado en que se realizará la auditoría.

Un programa de auditoría deberá contener los siguientes aspectos:

- Establecimiento de los objetivos en la revisión
- Determinación de los aspectos del sistema
- Definición de las tareas de la auditoría informática identificando sus jerarquías
- Planeación del desarrollo lógico de las tareas simultáneas y de su secuencia, así como las actividades respectivas
- Programación del trabajo de acuerdo al enfoque y alcance, estableciendo las fechas de terminación y restricción de actividades

Los proyectos sumamente complejos y cuyos requisitos de programación sean estrictos, requerirán de la técnica de sistemas de redes, identificando la ruta crítica de la auditoría.

Al organizar un programa de auditoría, conviene dar la importancia debida a la formulación de una política que señale objetivos y refleje un plan definido para la consecución de los mismos. Este plan debe incluir:

- La selección del personal apropiado para la ejecución de las tareas
- La determinación del procedimiento para realizar el trabajo
- El establecimiento de controles de avance y tiempos
- La revisión de los aspectos principales del sistema
- La preparación del informe incluyendo observaciones y deficiencias, así como las recomendaciones convenientes.

Los pasos que se seguirán en una auditoría informática serán principalmente:

1. Investigación preliminar
2. Elaboración del programa detallado de auditoría
3. Elaboración de cuestionarios y programación de entrevistas
4. Recopilación de la información requerida
5. Clasificación y análisis de la información recopilada
6. Elaboración del borrador del reporte preliminar y revisión interna de dicho reporte
7. Elaboración del reporte definitivo de la auditoría
8. Comentarios del reporte con las áreas involucradas y anexo de dichos comentarios al informe

3.2.3 Técnicas que se utilizarán en la Auditoría

La entrevista es la técnica más significativa y productiva de que dispone el auditor para recabar datos, consistente en un intercambio de información que se efectúa de persona a persona. Sirve para obtener información acerca de las necesidades y alternativas de solución a los problemas que se presentan.

Con el objeto de lograr el óptimo resultado en la entrevista, el auditor informático se apegará a los siguientes lineamientos:

a) Preparación de la entrevista.- Donde se deberá determinar la posición del entrevistado, se prepararán las preguntas que van a plantearse y los documentos necesarios a consultar, según sea el caso.

b) Conducción de la entrevista.- Donde se explicará el propósito del estudio al entrevistado, se harán preguntas especificas, evitando que exijan opiniones interesadas. Se deberá conservar el control de la entrevista, evitando las divagaciones y los comentarios al margen de la cuestión.

c) Secuencia de la entrevista.- Los pasos a seguir son: escribir los resultados, solicitar al entrevistado en caso necesario, su confirmación, correcciones o adiciones y archivar los resultados de la entrevista para análisis posteriores.

Otra de las técnicas de auditoría es la observación, la que podrá emplearse para verificar los resultados de una entrevista, o bien, como preparación para la misma. Se recomienda esta técnica para tareas cuantificables, relacionadas con la recopilación, acumulación y transformación de datos.

También deberá observarse la utilización que tengan los usuarios del sistema, la forma de operación, la frecuencia, etc.

El muestreo es un método estadístico que conduce a un conocimiento que se basa en las teorías estadísticas y en la ley de probabilidades. El valor del muestreo se aplica a los problemas que implicarían un enorme volumen de trabajo detallado, consistente en recoger y acumular datos para lograr un elemento de información, así como a operaciones que no es posible evaluar.

En muchos casos, el auditor necesita corroborar la existencia de ciertos datos o la confirmación de ciertos hechos, en donde se utilizará la técnica de la verificación.

El cuestionario es una herramienta de investigación y debe emplearse con cuidado. La estructura y contenido de un cuestionario debe incluir una explicación del propósito del mismo, instrucciones para su llenado, preguntas positivas y concisas.

La recopilación de documentos fuente, hojas de trabajo, informes, etc.. es otro medio para que el auditor obtenga información durante la primera fase de la auditoría. En estos documentos, el auditor podrá darse una idea de cómo esta estructurado el sistema, del funcionamiento actual, de qué elementos dispone, etc.

3.2.4 Desarrollo de la Auditoría

3.2.4.1 Investigación Preliminar

La investigación preliminar consiste en una revisión general a los principales aspectos de un sistema para determinar los problemas y situaciones de mayor importancia.

En esta fase se pretende obtener un diagnóstico previo del sistema, para que posteriormente, en la auditoría, se examinen y analicen profundamente los aspectos conflictivos del mismo, investigando sus causas y consecuencias.

Una investigación deberá dar la pauta para el desarrollo de la auditoría, ya que en base a ésta, se especificará su enfoque y alcance.

3.2.4.2 Elaboración de Cuestionarios y Entrevistas

Como ya se mencionó en las técnicas utilizadas en la auditoría, el cuestionario y la entrevista son las más útiles para el auditor, ya que por medio de ellas se puede conocer la problemática existente dentro del sistema, de una forma rápida y sencilla.

Es muy importante que dichas entrevistas se realicen con cada una de las áreas involucradas al sistema y que los cuestionarios sean adecuados a cada una de las mismas, conteniendo algunas preguntas iguales para obtener distintos puntos de vista.

Se recomienda que el número de preguntas no sea mayor de 40, para que se tenga el tiempo suficiente de aclarar cualquier duda que se presente en alguna de ellas.

Antes de iniciar con las entrevistas, es muy importante tener preparadas todas las preguntas que se harán en cada área. Si es necesario, se visitará nuevamente al entrevistado para realizar las preguntas derivadas de las entrevistas a las demás áreas.

3.2.4.3 Análisis de la Información Recopilada

En esta etapa se organizarán todos los resultados, resumiendo las respuestas obtenidas por cada una de las áreas, sobre los aspectos más importantes durante las entrevistas, incluyendo las observaciones objetivas por parte del auditor o auditores. Dicha información podrá ser enlistada de la forma más adecuada que el auditor lo considere.

El formato deberá contener los siguientes datos:

- Concepto, describiendo en pocas palabras el aspecto o problema;
- Punto de vista sobre el mismo, de cada una de las áreas a las que se investigó; y,
- Espacio para las observaciones.

Posteriormente, estas formas servirán para completar el informe de la auditoría, o si es necesario, anexarlas al informe definitivo.

Se recomienda que tanto los conceptos o problemas, como los puntos de vista de cada una de las áreas, sean expuestos en una forma clara y precisa. El número de columnas y hojas utilizadas, variará según las áreas y problemas o aspectos a considerar.

3.2.4.4 Recopilación de Documentos

Se recopilarán los principales documentos que componen el sistema, así como las formas impresas con las que opera.

Es importante consultar los manuales, guías, estudios, folletos, etc., que tiene el sistema para conocer su funcionamiento y su operación.

Después de analizar estos documentos, se deberá tener una apreciación sobre el uso que se les dé por cada una de las áreas que los utilizan, así como su intervención en los procesos.

Los documentos que no deben faltar en una auditoría de sistemas son:

a) Estudio o proyecto para la implantación del sistema

b) Manual del sistema

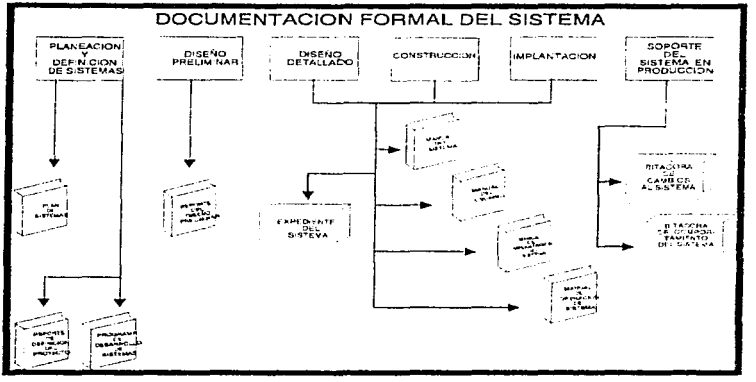
c) Manual del usuario del sistema

d) Manual de operación del sistema

e) Formatos de entrada de información

f) Formatos de salida de información

La documentación formal que todo sistema debe tener se muestra en la siguiente ilustración.



3.2.5 Informe de Auditoría

En el informe, el auditor requiere transmitir de una manera eficaz la información que ha obtenido en sus investigaciones y en la recopilación de documentos, de forma objetiva y fácil de entender.

Es conveniente que contenga una introducción con una breve explicación respecto a la finalidad de la auditoría del sistema.

Los aspectos que incluye un informe de auditoría son:

1) Generalidades.- Resumen de los hechos de mayor trascendencia, en orden de importancia y los hechos desfavorables que necesitan una acción correctiva.

2) Antecedentes del sistema.- Descripción breve de la historia del proyecto y/o sistemas, destacando los eventos principales y las áreas involucradas. Abarcará desde su origen, hasta la fecha de la auditoría, informando sobre la planeación, coordinación, diseño, desarrollo, implantación y evaluaciones del proyecto y/o sistema.

   Se especificarán fechas importantes, decisiones tomadas y compromisos adquiridos por las distintas áreas involucradas. En caso de existir reportes de avances, se deberán mencionar en esta sección.

3) Situación actual.- Constará de dos partes: la descripción del sistema y la descripción de la información que se maneja. En la primera parte, se describirá en forma breve el objeto del sistema, su utilidad, características generales, funcionamiento e integración.

   También se describirá el avance en el desarrollo del sistema, desde el punto de vista de actividades realizadas en base al programa y las necesidades satisfechas. Se especificará también el tiempo ocupado en cada fase de desarrollo del sistema, así como los problemas y sus causas en el avance.

   En la segunda parte, se describirá en forma general el tipo de información que se maneja, especificando su volumen e importancia, así como el avance en la carga, el uso y depuración de la misma.

4) Erogaciones.- Especificación de los costos de todo el proyecto, abarcando los costos y gastos de sistemas, equipo y personal.

Dentro de los sistemas deberán incluirse los costos y gastos correspondientes a la renta y/o compra e instalación de paquetes computarizados, así como los cursos impartidos al personal sobre el funcionamiento e implantación de los mismos.

Dentro del equipo se consideran los costos y gastos por concepto de renta y/o compra e instalación del equipo utilizado por el sistema, como: terminales, líneas telefónicas, modems, procesadores, etc. En caso de ser compartido con otros sistemas, se hará un prorrateo aproximado.

Es recomendable considerar dentro del aspecto de erogaciones por el personal que labora en el sistema, los conceptos correspondientes a sueldos, horas extras, capacitación especial, prestaciones y costos de asesoría externa en el caso de que se requiera.

5) Conclusiones.- Es la parte más importante del estudio porque refleja los puntos principales de la auditoría, los proyectos detectados y las recomendaciones o propuestas para el mejor funcionamiento del sistema.

En cada observación se especificará el hecho principal, su problemática, sus causas y efectos o consecuencias. Asimismo, se escribirán las recomendaciones, pudiendo proponer una sola solución para varias observaciones.

Estas recomendaciones necesitan especificar los medios que se utilizarán y la manera de llevarlos a cabo.

Al final del informe, se escribirá la fecha de elaboración (día, mes y año) y la persona responsable del estudio.

Para garantizar en la revisión final la correcta elaboración del informe, el auditor deberá plantearse las siguientes preguntas:

- ¿En el informe están contenidos todos los hechos de importancia?
- ¿Están presentados todos los aspectos en forma breve y es correcta la redacción del informe?

- ¿Está redactado el informe con suficiente claridad para que las exposiciones no sean mal entendidas?

- ¿Comprende el informe exposiciones claras respecto a la situación del sistema?

- ¿Están presentadas las observaciones y recomendaciones de una manera apropiada y elaboradas por medio correcto, conciso y cortés?

- ¿Se ha tenido objetividad y expresión correcta de ideas en el informe?

- ¿Se incluye toda la información necesaria de interés para el lector?

- ¿Las recomendaciones son oportunas, fáciles de realizar y convenientes a la organización?

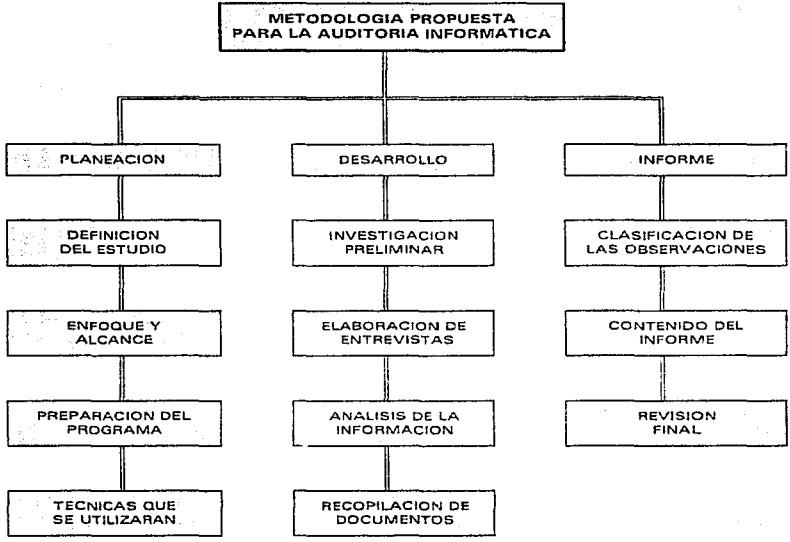
- ¿Lo tratado en el informe es interesante, bien redactado, comprensible y es realmente útil a la dirección y áreas involucradas?

- ¿La auditoría practicada fue llevada a cabo con profesionalismo y ética profesional?

Si el auditor puede contestar afirmativamente estas preguntas, podrá estar seguro de que el informe es correcto.

En todos los casos que sea necesario, se incluirán anexos al informe de: ilustraciones, costos, informes anteriores, etc.

El siguiente esquema ilustra gráficamente la metodología propuesta en este capítulo para desarrollar una auditoría informática.



CAPITULO IV

PLAN DE CONTINGENCIAS

4.1 Seguridad en los Sistemas de Información

La información es uno de los activos más importantes de una organización, si no el más importante; como tal, la protección de la información y de las instalaciones en que la procesan y almacenan es vital para el desarrollo de las operaciones. Las repercusiones de las deficiencias en la seguridad, se reflejan en negocios perdidos, reputaciones dañadas, pérdidas fiduciarias, pérdida de activos, etc.

Los controles de seguridad son necesarios para salvaguardar la información de modificaciones accidentales o no autorizadas, de destrucción y divulgación, y para garantizar su oportunidad, disponibilidad y utilidad.

Los conceptos actuales de seguridad de datos, son el resultado de tres factores que se interrelacionan: el avance de la tecnología de cómputo, la necesidad de procesar grandes cantidades de datos tan rápido como sea posible y la capacidad de cómputo para procesar desde lugares distantes a la computadora central.

La seguridad de la información automatizada, se puede considerar como la protección de todos los recursos (instalaciones, equipos y datos) contra daños naturales o provocados por el hombre.

El auditor en informática tiene como parte de sus funciones y responsabilidades, el evaluar la suficiencia de las medidas adoptadas para abatir la posibilidad de que los riesgos se materialicen, y en caso de que esto suceda, tener los controles adecuados que disminuyan la pérdida, agilicen la recuperación de la información y el restablecimiento de los sistemas.

Es preciso exponer que riesgo "... es el valor de la incertidumbre de que se presente un desastre o contingencia, medido en términos del número de amenazas posibles".[1]

---

[1] Cfr. Franco Romo, Alfonso, et. al., Planeación de la Recuperación Informática en Caso de Desastre, p. 9

Es decir, una acción o evento el cual puede causar una pérdida.[2]

Por lo anterior, es de suma importancia conocer los diferentes riesgos que amenazan un centro de cómputo y a la información que se procesa en él; estos se clasifican en dos grandes grupos:

- Riesgos externos.- Son todos aquellos que se presentan en el ambiente que rodea a una instalación de cómputo, como por ejemplo, temblor, inundación, sabotaje, motines sociales, robo, fraude, fallas de energía, etc.

- Riesgos internos.- Son los que se generan dentro de la propia instalación de cómputo, como por ejemplo, destrucción - voluntaria e involuntaria - de datos y recursos materiales, robo de material y/o de información, sabotaje, fraude, etc.

Una vez identificados y clasificados los riesgos, es importante conocer las medidas de seguridad que es necesario implantar, con el fin de minimizar su impacto en caso de que se presenten, garantizando la continuidad en el servicio.

Estas medidas, a su vez, se clasifican en físicas y lógicas:

- Seguridad física.- Contempla las medidas que permitan garantizar la integridad de equipos y recursos en el centro de cómputo, es decir, la protección de todo aquello que es visible y tangible. Desde el punto de vista computacional, " ... es la protección de hardware y software contra daños o destrucción, ocasionados por incendios, inundaciones o sabotaje".[3]

- Seguridad lógica.- Abarca las medidas que permitan proteger directamente la información contra su pérdida, modificación o divulgación, ya sea accidental o intencional, es decir, la protección de lo que se puede ver pero no tocar.

Sin embargo, es importante considerar que para que las medidas de seguridad, tanto físicas como lógicas cumplan su objetivo, es necesario establecer procedimientos administrativos adecuados.

---

[2] Weber, Ron, EDP Auditing, Conceptual Foundations and Practice, pp.248

[3] Sanders H., Donal, Informática: Presente y Futuro, p.538

Analizar las características de privacía, seguridad, disponibilidad e integridad de los servicios de cómputo, son tópicos de gran importancia. Cuando se habla de un desastre en computación, se debe fundamentalmente a un error de prevención, producto de poca o nula planeación.

En este capítulo de Plan de Contingencias, se señalan los puntos necesarios para planear y recuperarse de dichos desastres basándose en una adecuada planeación.

Actualmente, es indispensable considerar la planeación en la administración de los servicios de cómputo, con el objeto de contar con los procedimientos para el manejo de emergencias en casos de catástrofe o amenazas mayores para proteger al personal, minimizar el daño a las instalaciones y equipo de procesamiento de datos, así como para reducir la magnitud de la interrupción en el servicio.

Los procedimientos de emergencia se aplican a condiciones previas o poco después de una catástrofe y se ejecutan en situaciones obviamente no usuales; son de naturaleza temporal.

Estos procedimientos normalmente están contenidos en un documento que especifica, en términos claros, las políticas y actividades detalladas que deben realizarse en caso de presentarse un desastre o interrupción mayor del servicio, cualquiera que sea su causa.

Los planes de contingencia pueden definirse como *el elemento de control interno que es establecido para asegurar la disponibilidad de los datos valiosos de la computadora y sus recursos, en el caso de un evento que ocasione la interrupción de las operaciones.*

Un plan de contingencia detalla los procedimientos para establecer de forma rápida las capacidades de procesamiento de la organización cuando ocurre algún evento que provoca que las facilidades de procesamiento o de comunicaciones se vuelvan inoperables o inaccesibles.

Ya que en toda organización con servicio de cómputo resulta necesario mantener un alto grado de privacía, seguridad, disponibilidad e integridad en la información, se define un desastre o contingencia en computación, como aquel momento en que alguna de estas cuatro características se ve disminuida en la operación de la organización.

La definición anterior permite distinguir diferentes tipos de contingencias en función de la gravedad del caso:

a) Contingencia menor. Es aquella que no tiene repercusiones fundamentales en la operación diaria y es normalmente recuperable en menos de tres o cuatro horas.

b) Contingencia grave. Es aquella que no afectará significativamente la operación de la organización, pero que resulta recuperable, si se han tomado las debidas normas preventivas, en 24 o 48 horas.

c) Contingencia crítica o fatal. Similar a la anterior, sólo que no es recuperable, ya sea porque no existen normas preventivas, o bien, por que las existentes no son suficientes.

Debe quedar claro que aunque resulta imposible evitar contingencias, lo que es necesario es que éstas no caigan en la categoría del inciso c).

Con respecto al tipo de contingencias, éstas se pueden clasificar como:

- Contingencias en el procesador central. Cuando los procesos de la información fallan.
- Contingencias en las comunicaciones. Cuando la comunicación de la información falla.
- Contingencias en la información. Cuando lo que falla es la base de datos, pérdida de un archivo, etc.
- Contingencias en la instalación. Cuando se detecta fuego, la ruptura de una tubería, etc.

Esta clasificación es importante, ya que inclusive en la vida diaria se suele decir que existen problemas de comunicación, cuando en realidad se tienen problemas de proceso, esto es, los datos llegan a donde deben, sólo que la gente no toma las decisiones correctas.

Referente a las repercusiones de las contingencias, éstas se pueden clasificar en:

- Contingencias en el hardware.- Daños en el equipo físico
- Contingencias en el software.- Pérdida de archivos

Referente a las causas de las contingencias imputables al recurso humano se tiene:

- Contingencia accidental.- Debido a errores u omisiones de los operadores o usuarios de un sistema.
- Contingencia intencional.- Como un ataque directo o con intención predeterminada de dañar a la organización.

4.2 Planeación para la Recuperación

Por más protección que se tenga, los desastres ocurren, por esta razón resulta necesario planear una metodología de recuperación para todos y cada uno de los casos de desastre mencionados.

Sin una verdadera planeación, resultaría imposible llevar a cabo una recuperación. Así por ejemplo, aún contando con un sistema de respaldo de datos y programas, en caso de una falla en el hardware, el problema puede ser crítico si no se cuenta con una instalación alterna donde se puedan correr los programas.

Asegurar la continuidad de las operaciones de la organización es el objetivo principal de la elaboración de planes de contingencia y en el caso de sistemas es de especial importancia, ya que en ellos se basan muchas de las operaciones críticas de las organizaciones. Unas operaciones pueden ser críticas y otras aún no requerir de procesamiento en caso de desastre.

La pérdida potencial depende del tipo de interrupción en que se incurre y en la determinación del valor de los activos o funciones para la organización. Se debe estimar una pérdida potencial para cada área de riesgo.

La pérdida potencial de los activos físicos es igual a su costo de reemplazo, más el costo del retardo del procesamiento y el costo del salario de los empleados que trabajaron tiempo adicional. Los siguientes tipos de activos físicos deben ser incluidos dentro de la estimación de pérdida potencial.

- Hardware (CPU[4], unidades de memoria, periféricos, terminales remotas, controladores, equipo y líneas de comunicaciones, impresoras y cualquier otro tipo de hardware)
- Equipo auxiliar que da soporte al centro de procesamiento (como aire acondicionado, modems[5] y equipo de regulación de energía eléctrica)
- Consumibles (cintas, diskettes, papel, toner, etc.) y equipo de oficina
- El edificio que da alojamiento al centro de cómputo

Un plan de recuperación empieza con la formación de un Comité de personal responsable de manejar las contingencias, que identifique y defina lo siguiente:

- Las acciones que deberán tomarse en caso de una contingencia.
- Las necesidades mínimas de supervivencia operativa.
- Las relaciones con instalaciones de respaldo.
- La instrumentación de planes.
- Establecer lineamientos para determinar la naturaleza y nivel de la catástrofe, incluyendo las instrucciones que deben seguirse según la clase de desastre identificado.
- La reglamentación para la observancia de las normas de prevención.
- La definición de respaldos y frecuencia de los mismos.
- La elaboración de los manuales de emergencia y recuperación.

---

4 Siglas de "Central Processing Unit", Unidad Central de Procesos.

5 Yuxtaposición de Modulador/Demodulador. Dispositivo que convierte señales digitales desde una terminal (o PC) a una señal adecuada para transmitirse en un canal telefónico (analógico). En el otro extremo, otro modem convierte la señal analógica en digital, y la transmite a la computadora de ese extremo.

- El establecimiento de personal mínimo de guardia para la recuperación.
- La definición de políticas de respaldo de la información automatizada.

Para determinar las necesidades mínimas de supervivencia operativa, resulta conveniente definir los trabajos del centro de procesamiento de datos en tres categorías básicas:

a) Prioridad alta.- Aquellos que están sujetos a fechas de entrega límite y de cuya ejecución depende la organización, comúnmente a esta información se le llama vital.

b) Prioridad media.- Trabajos críticos para la organización, pero que puedan retrasarse.

c) Prioridad baja.- Aquellos que no son críticos y cuya fecha de entrega puede posponerse.

Para planear la recuperación en caso de contingencias usando esta clasificación propuesta, se definen solamente aquellos desastres a los que está sujeta la organización, ya que considerar todos los desastres sería imposible e incosteable y se proponen soluciones concretas a cada uno de ellos para su posterior recuperación. En caso de una emergencia, no se requieren manuales con toda la información a detalle, únicamente se piden líneas de acción para el caso específico.

En virtud de lo anterior, se selecciona la mejor propuesta por cada desastre y se procede a generar un manual que explique la teoría para instrumentar la recuperación. Una vez instrumentado el plan, se procede a simular efectivamente cada caso y adquirir información para retroalimentar los planes.

Es importante mencionar que una buena simulación puede llevarse a cabo en la organización, transportando los archivos diarios a una instalación alterna con el fin de no parar la producción de la organización y luego conducirse en la instalación como si hubiese sucedido un desastre; esto es, hacer un simulacro del desastre.

Es responsabilidad del Comité entablar relaciones con centros de operación alternos; en algunos casos, será necesario entablar relaciones contractuales y una vez establecidas, desarrollar paquetes de conversión de sistemas en caso de tener versiones diferentes de los sistemas operativos.

En el caso de un desastre, el Comité debe designar un grupo de personas de guardia para poder atender inmediatamente la recuperación del sistema. En cualquier caso, el personal de guardia deberá tener copia del manual de contingencias, en el cual se deben especificar todas y cada una de las acciones a tomar en caso de una emergencia.

4.3 Manual de Contingencias

Los componentes mínimos del manual de contingencias deben ser:

- Procedimientos iniciales de avisos y acciones.
- Lista de personas que puedan arrancar un plan de desastres y de los coordinadores responsables de la centralización de la información durante la emergencia, que deben ser informadas de manera inmediata.
- Requerimientos de personal para la recuperación.
- Direcciones y teléfonos de:

  - Centro alterno
  - Proveedores
  - Clientes
  - Personal
  - Servicios médicos
  - Policía
  - Servicios de emergencia

- Rutas de transportación primaria y alterna en el caso que resulte necesario enviar a los empleados a su domicilio
- Procedimientos para activar el equipo de soporte
- Mecanismos de notificación y control de actividades
- Operaciones a procesar en el centro de apoyo o facilidades alternas
- Prioridad de operación de sistemas, separando lo vital de lo importante.

- Planes de evacuación y planes alternos en caso de fuego, bomba o explosión
- Procedimientos para solicitar la asistencia de la policía y de los bomberos
- Procedimientos de recuperación, conmutación telefónica y restauración de los servicios del centro de cómputo
- Reporte y evaluación de riesgos existentes en el centro de procesamiento de datos
- Copias de contratos y seguros de mantenimiento y respaldo
- Mecanismos de respaldo existentes, guardando la versión "abuelo" de cintas en un lugar aparte del centro de procesamiento de datos

Conviene mencionar que este manual debe existir tanto en la instalación como en otros lugares, aunque en forma restringida, sólo personal del Comité o de guardia deberá tener acceso a él.

El manual debe ser un documento con vida, esto es, dinámico, porque se deberá modificar cada vez que ocurra alguno de los siguientes hechos:

- Cambio de personal
- Cambio de equipo o instalación
- Cambio de teléfonos
- Cambio de sistemas
- Cambio en las condiciones socio-políticas de la ciudad/país
- Cambio de contratos de mantenimiento
- Cambio en las pólizas de seguros
- Cambio en las instalaciones de respaldo y alternos

Se requieren instrucciones detalladas y completas para los siguientes aspectos:

- Ubicación de los procedimientos de emergencia.
- Ubicación de la lista de teléfonos de los ejecutivos clave y de emergencia tales como: el administrador de la base de datos, administrativos y de relaciones públicas; policía, bomberos, ambulancias y hospitales.

- Definición del criterio de evacuación en caso de que la autoridad apropiada no se haya localizado.
- Estaciones de trabajo emergentes o facilidades alternas.
- Minimizar el daño de archivos importantes y equipo.
- Obtención de servicio de emergencia o procesos especiales y adquisición de materiales.
- Lineamientos para el arreglo y obtención de transportación especial.
- Desarrollar una lista de equipo, registros y áreas que deberán ser protegidas con la mayor prioridad.
- Estimar la duración más probable de la interrupción según el tipo de emergencia.
- Programar las pruebas y revisión periódica de los componentes del plan de contingencias.

Finalmente, cabe destacar que, aunque el Comité de contingencias es quien define y regula el desastre y la recuperación de la instalación, la responsabilidad de dicha operación deberá recaer y ser aceptada por el responsable del centro de cómputo, quien deberá formar parte del Comité.

Para la recuperación de desastres graves, el Comité deberá ser convocado para definir la ruta de acción a seguir, no en forma espontánea, sino usando el manual que para su efecto debe existir.

Tan pronto como ocurra el desastre, será necesario definir las consecuencias y alcances del mismo, enseguida deberá entablarse comunicación con los usuario/clientes, proveedores y responsables del equipo, así como con la instalación externa de apoyo donde se espera procesar temporalmente los sistemas de alta prioridad de la organización.

Normalmente será necesario anotar y registrar las causas y consecuencias inmediatas del desastre, para poder iniciar toda la tramitación legal del pago de seguros, deslinde de responsabilidades, etc.

Es importante mencionar que el plan de contingencias debe contemplar anticipadamente dos opciones básicas:

- Operación temporal sin recuperación total
- Recuperación alterna y total a largo o mediano plazo

En ningún momento se deben mezclar estas dos actividades, ya que las del primer caso aseguran la supervivencia operativa y deben ser consideradas aparte. La recuperación alterna debe ser hecha sin prisa y tal vez demande actividades que lleven tiempo como son:

- Reconstrucción
- Cobro de primas de seguro
- Reprogramación

Entre los imperativos básicos para la puesta en marcha del plan de contingencias se pueden citar los siguientes:

a) Verificar la imposibilidad de operación básica en la instalación. Sólamente en caso afirmativo se debe proceder al uso de la instalación alterna.

b) Revisar los requerimientos de compatibilidad de equipo en la instalación alterna. En caso de existir modificaciones significativas, por ejemplo, trabajar en sistemas operativos diferentes, deberán estar grabados programas ya convertidos en cintas de apoyo con el fin de reducir el tiempo de instalación del sistema en la instalación alterna.

c) Revisar los procedimientos de seguridad, privacia y planes de contingencias en la instalación alterna, con el fin de evitar un doble desastre que sería crítico e irrecuperable.

   Este imperativo es fundamental en el aspecto de privacía, sobre todo si se encuentra que la instalación alterna tiene usuarios completamente ajenos. Un desastre por falta de privacía debería ser considerado tan grave como el desastre que obligó al uso de la instalación alterna.

Sobre este aspecto conviene modificar los passwords*, uno al moverse a la instalación alterna y el segundo al regresar a la inicial.

Las claves de acceso, contraseñas o caracteres magnéticos (passwords) sirven para:

- Permitir el acceso a personal previamente autorizado a estaciones de trabajo conectadas a la computadora central.

- Restringir el acceso a recursos de cómputo (archivos, bibliotecas, programas, procedimientos, etc.), ya sean residentes en disco o en cintas magnéticas, además de identificar el tipo de acceso permitido (lectura, actualización, borrado o creación).

Cuando en el sistema está activada la seguridad por claves de acceso, cada usuario debe proporcionar al sistema la identificación que tiene asignada, llamada también User-Id y su contraseña en la pantalla de inicio de sesión.

El User-Id identifica al personal que inicia una sesión en el sistema. Cada User-Id debe ser único. El sistema comprueba también la contraseña, la cual no se visualiza en la pantalla mientras el personal la teclea ni debe imprimirse en un proceso, cada contraseña también debe ser única. Recomendamos no atenerse a un esquema reconocible para la asignación de contrasoñas, como fechas de nacimiento o números de la extensión telefónica, pues resultaría fácil para otras personas el averiguarlo; las contraseñas, por consiguiente, deberán ser aleatorias y de grupos de caracteres no significativos.

El cambio de contraseña deberá realizarse al menos cada 60 días, pero si se sospecha que alguien conoce la contraseña de otro usuario, deberá cambiarse inmediatamente, o bien establecer un procedimiento interactivo que permita mantener la confidencialidad y seguridad en las claves de acceso o passwords, lo cual da la facilidad al personal de poder cambiar periódicamente sus claves de acceso con la frecuencia que sus necesidades lo requieran.

La contraseña debe ser personal e intransferible, cada usuario es responsable del buen o mal uso de la que le corresponde, por lo que deben ser motivados a protegerlas y no a compartirlas o revelarlas.

---

* Autorización para permitir el acceso a información o procesos por medio de una señal o clave, conocida únicamente por los individuos autorizados.

Para tener acceso a recursos protegidos por claves de acceso, es necesario establecer perfiles de usuarios por recursos, los cuales entre otros atributos deben contener:

- Nombre del usuario
- Area a la que pertenece
- Tipo de acceso
- Privilegio
- Vigencia de acceso

4.4 Documentación del Plan de Contingencias

El éxito de la planeación de contingencias está directamente relacionado con la calidad de su documentación. La estructura del documento debe facilitar su entendimiento, su implementación y su mantenimiento.

A continuación se comenta la documentación típica para estos casos:

Equipos de restablecimiento.- La composición y responsabilidad del equipo debe estar claramente documentada con nombres, direcciones y teléfonos del trabajo y del domicilio, plaza, uso y funciones dentro del equipo, área de responsabilidad, etc.

Composición y funciones.- El equipo debe estar compuesto de profesionales que estén calificados para realizar un restablecimiento en caso de falla.

Plan de acción de restablecimiento.- Debe incluir planes generales y detallados para las actividades específicas que deben realizarse. Este plan documenta las actividades que deben ocurrir en una base "hora por hora" y las responsabilidades para la realización de estas actividades.

Recobro de registros vitales.- Contiene una lista de los archivos críticos que deben recuperarse para continuar con el procesamiento y procedimientos de recobro de esos archivos en cintas y discos de respaldo.

- Provisiones para respaldo fuera de lugar, realizando rotaciones de los recursos críticos y no críticos (sistemas operativos, aplicaciones, bibliotecas, etc.)

- Frecuencia de respaldo fuera de sitio y número de grupos de generación que se mantienen de los archivos de producción

- Etiquetación de los respaldos

- Pruebas periódicas para tener la seguridad de que los respaldos son los adecuados

Estos procesos no deben ser ni tardados ni complejos.

Procedimiento para las aplicaciones.- El plan debe enfatizar de forma clara la secuencia (prioridades) en las cuales deben restaurarse las aplicaciones y debe señalar los siguientes aspectos:

- Mecanismos automáticos para pasar los jobs a los sitios alternos de proceso y su prioridad

- Pasos para restaurar un sistema a partir del último respaldo disponible

- Procedimientos para atender las aplicaciones hasta que se restaure el servicio de la computadora

- Restaurar las aplicaciones a partir del sitio alterno

Para cada aplicación crítica el plan debe documentar lo siguiente:

- Una explicación de por qué fue considerada la aplicación como crítica

- Los componentes de la aplicación: nombre de la aplicación, identificadores de los programas, fallas, versión, código fuente y objeto y volúmenes en los que se encuentra contenido.

- Ubicación exacta del respaldo de la aplicación, archivos en producción y documentación

- Equipo, comunicaciones, software requerido por la aplicación

- Requerimientos mínimos de procesamiento
- Requerimientos de respaldo, incluyendo en sitio y fuera de sitio
- Requerimientos de seguridad y de control de acceso

Configuración del sistema operativo.- El plan debe contener un inventario de todo el software de sistemas que es necesario para reconstruir las aplicaciones. Dicho inventario debe incluir: nombre y tipo de software, versión, fecha de actualización, nombre del vendedor y dirección, provisiones tomadas para los respaldos fuera de sitio tanto del software como de su documentación.

Inventario del equipo del centro de proceso.- El inventario de todo el equipo necesario para reconstruir el centro de datos y dar soporte a las operaciones críticas debe incluir lo siguiente: configuración incluyendo el CPU y controladores de discos y cintas, terminales, controladores de telecomunicaciones, impresoras, suministros de energía eléctrica, unidades de enfriamiento, controles de humedad y otros periféricos, requerimientos de cableado y suministros de energía eléctrica, marca, modelo y modificaciones necesarias, capacidad, vendedor del equipo, espacio básico, luz necesaria y aire acondicionado.

Requerimientos de telecomunicaciones.- Debe incluir la configuración (swiches, multiplexores[7], concentradores, dispositivos de diagnósticos, controladores de comunicaciones y líneas de comunicación); descripción de la velocidad, amplitud de banda, número de identificación de circuitos de los canales de comunicación; proveedores; provisiones de respaldo incluyendo contratos con la compañía de teléfonos.

Pruebas del plan de contingencias.- Debe describir los planes de pruebas, incluyendo los objetivos de las pruebas, alcance, secuencia, documentación de los resultados y estimaciones de tiempo.

---

[7] Dispositivo capaz de enviar varias señales por el mismo medio, variando en cada una de estas señales, algún parámetro para diferenciarla de las restantes.

Facilidades de procesamiento alterno.- Debe incluir los detalles relacionados con el procesamiento alterno, específicamente acuerdos formales especificando lugar, duración del acuerdo, facilidades, espacio de oficina acordado y seguridad.

Formatos y proveedores.- El plan de contingencia debe documentar cualquier requerimiento de formas especiales, insumos y servicios necesarios para continuar con la operación de las aplicaciones críticas.

Las tareas logísticas de relocalizar sistemas de información dentro de marcos de tiempo realmente cortos debe señalarse cuidadosamente. Deben establecerse procedimientos alternos para recolectar las entradas y distribuir la salida.

Transportación y logística.- Las tareas más significativas en la planeación es la verificación y validación del plan. Estas actividades permiten que el plan sea constantemente analizado, discutido y ejecutado para que el equipo esté en estado de alerta.

El plan de contingencias debe procurar a la organización los siguientes beneficios:

- Verificar que el plan sea completo y práctico
- Determinar la factibilidad y compatibilidad de las facilidades de respaldo con los procedimientos
- Identificar y corregir las debilidades del plan
- Proporcionar entrenamiento al departamento de sistemas y de usuarios sobre los procedimientos de respaldo
- Incrementar la confianza de la organización en su habilidad para restablecerse
- Proporcionar una fuerte motivación para mantener el plan

Un plan de contingencias debe ser flexible y documentado de forma dinámica, y para que sea exitoso es indispensable que sea probado, evaluado y monitoreado frecuentemente. De otra manera, una organización no puede asumir que funciona.

Riesgos y controles.- El mayor riesgo asociado con la planeación de contingencias es que la disponibilidad de la información de los sistemas críticos pueda estar comprometida. Se incurre en este riesgo como un resultado de lo siguiente:

- La ausencia de un plan de contingencias
- Un plan diseñado pobre o inadecuadamente
- Un plan probado y evaluado incorrectamente

El análisis de riesgos es una herramienta que puede usarse para identificar amenazas relevantes y su impacto potencial en la empresa.

- **Riesgos:**
  - Inhabilidad para continuar con las operaciones
  - Pérdida o disminución de flujo de efectivo
  - Pérdida de ventaja competitiva
  - Pérdida de la cartera de clientes o compartir el mercado
  - Incremento de los costos
  - Multas y sanciones

- **Controles:**
  - Desarrollo y documentación del plan
  - Actualizaciones regulares del plan
  - Pruebas regulares del plan
  - Simulacros
  - Comunicación entre el equipo encargado del plan

4.5 Consideraciones de Auditoría

Los objetivos que persigue una auditoría a un plan de contingencias son los siguientes:

- Especificar y evaluar si el plan es adecuado
- Identificar las áreas potenciales de exposición en el plan
- Revisar las provisiones, procedimientos y staff que soporta la recuperación de una falla generalizada.
- Aportar recomendaciones detalladas para remediar las exposiciones detectadas

Estos objetivos son alcanzados a través de una revisión de los contenidos del plan y una prueba completa.

Revisión de los Contenidos del Plan.-

El auditor debe revisar que el plan esté completo, exacto, actualizado, adecuado y apropiado, incluyendo lo siguiente:

- Objetivos
- Definición y provisiones de los distintos niveles de fallo
- Que los escenarios estén documentados para cada nivel de falla
- Instrucciones de cuándo y cómo activar y usar el plan
- Procedimientos detallados y guías para cada área de restablecimiento
- Requerimientos de seguridad para alternar medios ambientes de procesamiento
- Distribución de los planes de contingencias al personal autorizado

- Revisión y aprobación de las provisiones por parte del administrador
- Identificación del personal clave del plan, incluyendo su responsabilidad en el mantenimiento del plan

Exactitud.-

El plan de contingencia debe revisarse en cuanto a la exactitud de sus puestos, configuraciones de hardware y software, staff, riesgos, requerimientos legislativos y de regulación.

Que el plan sea adecuado y apropiado.-

Para determinar que tan adecuado y apropiado resulta el plan, el auditor debe revisar lo siguiente:

- Composición y funciones del equipo encargado del plan
- Prioridades aplicadas para software y datos
- Inventario de equipo y configuraciones críticas
- Requerimientos de comunicación
- Inventario del software de sistemas y configuraciones críticas
- Formatos críticos y suministros necesarios
- Provisiones de respaldo para software, archivos y suministros
- Facilidades alternas de procesamiento
- Staff y sus asignaciones
- Inventario de transportación y logística
- Provisiones de seguridad
- Pruebas del plan de contingencias
- Cobertura de los seguros

Finalmente, podemos enfatizar que al depender cada vez más las organizaciones de sus sistemas de información para las operaciones críticas y aumentar el uso de las comunicaciones, crece la necesidad de contar con planes de contingencia.

Dicha necesidad se sustenta principalmente en:

- El reconocimiento de la información como un valioso activo de la organización
- El amplio uso de microcomputadoras y terminales en los departamentos de los usuarios
- La dependencia de las organizaciones en las computadoras
- Crecimiento de los procesamientos en línea y tiempo real

Es por ello que concluimos que el principal objetivo de la elaboración de un plan de contingencias, es asegurar que la capacidad de procesamiento de la información en la organización se reanude lo más rápidamente posible después de una interrupción derivada de un suceso desastroso, a fin de salvaguardar los bienes institucionales.

CONCLUSIONES

En un principio, la auditoría informática se limitaba a verificar que los sistemas que operaban en equipos de cómputo cubrieran ciertas características de seguridad, exactitud, integridad, peso, etc. En nuestros días la auditoría informática ha expandido sus campos de acción; ya no sólo se enfoca al uso de computadoras, sino a todo lo que se refiere a sistemas de información, a verificar que una función de informática apoye realmente los objetivos de una organización, que sea eficiente y esté acorde con los lineamientos y con la misión de la empresa. Es decir, de un esquema micro, que era un aspecto muy técnico y básicamente relacionado con estados financieros, podemos decir que ahora es una función con mucho más peso dentro de las organizaciones.

La auditoría informática consiste en evaluar y asegurar que la función de informática dentro de la organización esté cumpliendo con sus objetivos de apoyo a la misión de la empresa y que los recursos sean utilizados en forma eficiente. Ya no hablamos únicamente de que se cuente con información periódica correcta y oportuna, sino del uso de la tecnología como soporte a la operación y a los servicios que se brindan.

Los bancos son un caso muy representativo: los cajeros automáticos, el banco en su casa o el banco en su empresa, son un ejemplo de que ya no se trata sólo de asegurar que el estado financiero cuadre o esté completo, sino de que se esté utilizando la tecnología en apoyo a los objetivos de una misión.

Uno de los grandes beneficios que nos proporciona la auditoría, es saber que la inversión en informática de una empresa está redituando en forma correcta; que la inversión que se hace en recursos informáticos está teniendo un retorno satisfactorio.

En esta época se habla mucho de mejorar la productividad, de reducir costos, etc. La función informática juega un papel crítico en este caso, porque ayuda precisamente a ser más eficientes, a reducir costos sin demérito ni de la cantidad, ni de la calidad de los servicios o productos que se generan.

Por otro lado, existen dos tipos de revisión para determinar la frecuencia adecuada en la aplicación de la auditoría informática. La primera es la revisión de la infraestructura informática, que en el acuerdo de auditorías se llama *revisión de controles generales*. Es decir, se revisa cuál es la estructura con que se cuenta, si el personal es el adecuado, si los procedimientos son correctos, que existan adecuadas medidas de seguridad, tanto seguridad física de los equipos, como seguridad de acceso a la información.

Una vez teniendo la certeza de que esta infraestructura es la adecuada, se comienza la revisión de la información sobre la funcionalidad de los sistemas y de las aplicaciones que existen. Por ejemplo, en una compañía de Seguros, una vez que se ha revisado su equipo de cómputo, la organización del departamento, los recursos humanos, etc., se comienza a analizar la operación de los sistemas, cómo funcionan, que la información sea correcta y oportuna, que los recursos sean utilizados eficientemente y en forma consistente.

Estas revisiones son periódicas, pero dependen de que tan importante o que tanto impacto tengan los sistemas de información en las organizaciones para definir una periodicidad general. Hay empresas que no dependen en un alto grado de sus sistemas de cómputo porque muchas actividades se realizan de forma manual; en este tipo de empresas es un poco más holgada la necesidad de hacer revisiones.

En suma, podemos decir que en una revisión inicial se evalúa la infraestructura y después deben realizarse revisiones periódicas al funcionamiento de las aplicaciones. Estas revisiones pueden ser desde bimestrales, semestrales, etc., hasta tener una participación continua de auditoría en forma consistente para aquellas aplicaciones críticas.

En México tenemos muchas oportunidades de perfeccionar las funciones administrativas de las empresas para hacer mejor las cosas, en menor tiempo y a menor costo, y la informática puede jugar un papel determinante en este propósito.

Es aquí donde cobra importancia la participación del auditor, porque es la persona que puede evaluar una situación y recomendar cambios y mejoras. El auditor no es quien va a criticar o descubrir culpables, sino quien dará sugerencias constructivas y ayudará a mejorar el estatus de trabajo.

El examen de los procedimientos de auditoría y sus relaciones con los conceptos de existencia y valoración, nos lleva a la conclusión de que el papel de los sistemas de cómputo afecta en forma muy significativa a las técnicas de auditoría.

El uso de la computadora para evaluar la calidad del sistema de procesamiento de datos y determinar la validez de la información generada, proporciona al auditor la oportunidad de ejercer un análisis más profundo del cuantioso volumen de transacciones.

De esta manera, se ha reflexionado brevemente sobre el problema de riesgos y controles en ambientes de cómputo, pero las expectativas para el futuro son cada vez más complejas y, por tanto, la auditoría informática también.

El desarrollo de la presente investigación ha perseguido ser una contribución, que basada en diversas metodologías auxilie a la dirección de las organizaciones, para asegurar el adecuado uso de sus sistemas, a partir de una dinámica que pueda aplicarse en beneficio de la gestión de informática.

Finalmente, sólo nos resta manifestar que con este bosquejo se pretende mostrar la forma en que la tecnología empleada en las organizaciones afecta nuestra profesión, ya que para mantenernos en el mercado y para superar el nivel de nuestros servicios, es necesario tener conocimientos de una gran variedad de materias altamente técnicas como es la auditoría, tanto por nuestra iniciativa, como por las propias necesidades de la empresa, que por su tamaño, por las operaciones que maneja, por la responsabilidad ante sus clientes y por la diversificación de su mercado, es de capital importancia contar con información oportuna, confiable y a un costo moderado, lo que ha provocado que se utilice la tecnología de la informática para agilizar este proceso.

ANEXO

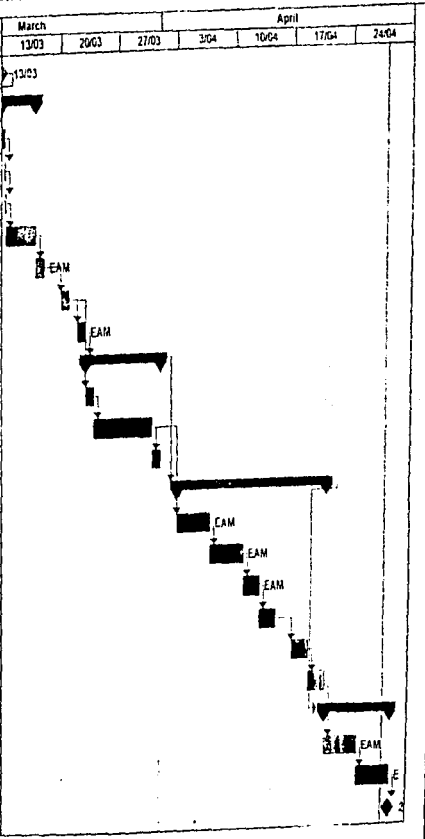
A continuación se muestra un ejemplo de una auditoría aplicada al sistema de Recibidor de Materiales en una Compañía de Bienes de Consumo.

ÍNDICE

1.- PLAN DE TRABAJO

Programa de trabajo
Recepción de Materiales

ID	Task Name	Duration	Start	Finish
1	Inicio	0d	13/03/95	13/03/95
2	Introduccion al módulo	4d	13/03/95	16/03/95
3	origen del modulo	0.2d	13/03/95	13/03/95
4	objetivo	0.2d	13/03/95	13/03/95
5	motivación	0.2d	13/03/95	13/03/95
6	documentación	3.4d	13/03/95	16/03/95
7	Analisis del ambiente desarrollo	1d	17/03/95	17/03/95
8	Análisis flujo de información	1d	20/03/95	20/03/95
9	Entrevistas a usuarios	1d	22/03/95	22/03/95
10	Analisis de interfases	7d	23/03/95	31/03/95
11	diagrama de flujo	1d	23/03/95	23/03/95
12	revision detallada	5d	24/03/95	30/03/95
13	deteccion de inconsistencias	1d	31/03/95	31/03/95
14	Analisis del de funciones	14d	3/04/95	20/04/95
15	Recepción de materiales	4d	3/04/95	6/04/95
16	Devolución de materiales	2d	7/04/95	10/04/95
17	Cancelación de recepciones	2d	11/04/95	12/04/95
18	control de calidad	2d	13/04/95	14/04/95
19	consultas	2d	17/04/95	18/04/95
20	reportes	2d	19/04/95	20/04/95
21	Plan de optimización del módulo	6d	21/04/95	28/04/95
22	Relación de problemas	2d	21/04/95	24/04/95
23	Sugerencia de solución	4d	25/04/95	28/04/95
24	Fin	0d	28/04/95	28/04/95



2.- INTRODUCCIÓN AL SISTEMA

2.1 ORÍGEN:

Originalmente la aplicación de "Recepción de Materiales" se controlaba en dos equipos, una parte en PC, y la otra en el equipo AS/400. Para facilitar el uso y manejo de información de todos los usuarios involucrados, se decidió desarrollar el sistema totalmente en el AS/400.

2.2 OBJETIVO:

El objetivo del Sistema es llevar el control de la recepción de materiales para producción, dicho Sistema se compone de los siguientes módulos:

Recepción de Materiales
Confirmación de la Recepción de Materiales
Cancelación de la Recepción de Materiales
Devolución de Materiales a Proveedor
Control de Calidad
Afectación a otros Sistemas
Consultas
Reportes

2.3 JUSTIFICACIÓN:

El nuevo Sistema de Recibo de Materiales a presentado desde el inicio de su operación, diversos problemas de inconsistencia en los resultados finales para lo cual, se realizan modificaciones a los programas y se corrige la información, en otros casos, sólo se corrige la información sin antes detectar la causa de tales problemas agregando esta actividad a las propias del cierre mensual, resultando esto el orígen del presente proyecto.

2.4 DOCUMENTACIÓN:

a) *Manual de Usuario*: Tiene dos omisiones:
   la explicación del proceso de cambio de turno y,
   los mensajes de error y sus acciones a ejecutar.
b) Manual Técnico: Esta incompleto:
   falta el flujo de datos,
   la interrelación con otros sistemas y,
   mensajes de error y sus acciones a ejecutar.
C) *Documentación de Programas*: Contiene en general los comentarios necesarios excepto, en las modificaciones. No se lleva una bitácora de los cambios efectuados.

3.- AMBIENTE DE DESARROLLO

Control de fuentes:
No existen ambientes separados para desarrollo y producción, en lo que a fuentes se refiere.
Para realizar un cambio a un programa que está en producción, el programador hace una copia del fuente, con el mismo nombre, pero, agregándole un sufijo: ("BK", "BK1", "BK2", "XXX", etc.). Las modificaciones las hace sobre el fuente original; lo anterior puede provocar inconsistencias entre fuentes y objetos que están corriendo.

RECOMENDACIÓN: Se sugiere crear los ambientes necesarios para separar el ambiente de producción y desarrollo, así como generar una aplicación que controle las liberaciones, llevando además, un control de los fuentes y objetos correspondientes, esto apoyado de formatos, políticas y procedimientos.

Documentación interna:
El personal de programación desarrolla sus cambios sin documentar el motivo, sus iniciales, las fechas, etc.

RECOMENDACIÓN: Se comentó con la Lic. Esperanza Sánchez y se acordó que se inicie este tipo de documentación interna.

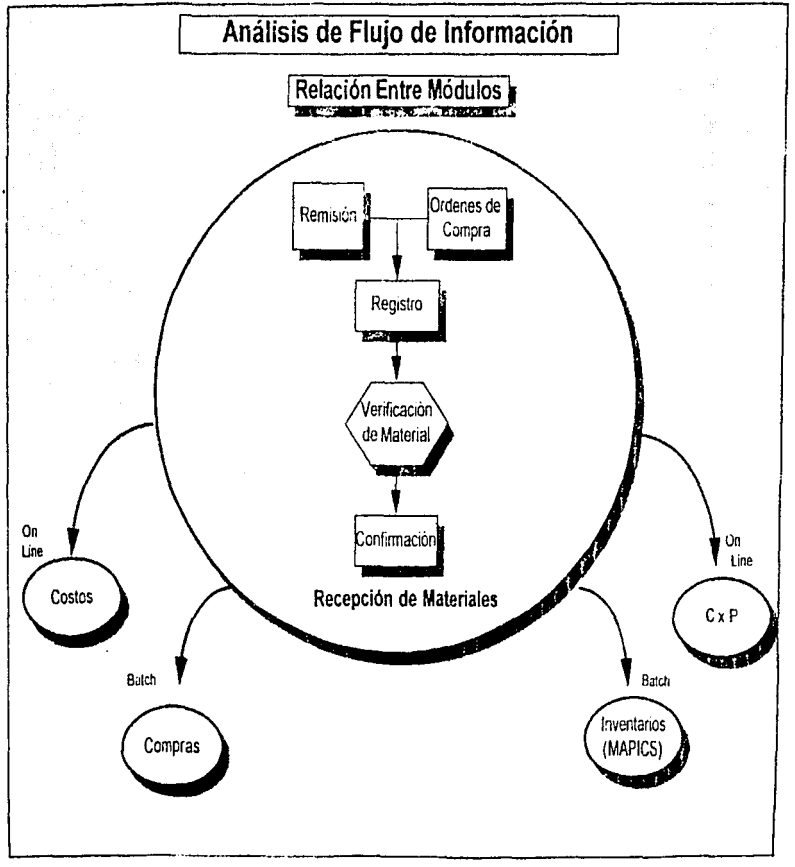
Control de calidad:
No existe control de las modificaciones efectuadas a un mismo programa, no se sabe cuántas liberaciones lleva un programa por un mismo requerimiento, debido a que el responsable de la modificación no se auxilia del usuario para hacer pruebas exhaustivas del programa en ambiente de desarrollo antes de que se libere y, por lo tanto, esta prueba se realiza en producción.

RECOMENDACIÓN: Se sugiere implantar un formato de Vo.Bo. por parte del usuario y del coordinador de sistemas antes de la liberación, y solo hasta obtener estos Vo.Bo's el área de operación (Centro de Computo) acepte las liberaciones

4.- ANÁLISIS DE FLUJO DE INFORMACIÓN

Diagrama de relación entre módulos

Se anexa documento


Análisis de Flujo de Información
Relación Entre Módulos
Remisión
Ordenes de Compra
Registro
Verificación de Material
Confirmación
Recepción de Materiales
On Line
Costos
Batch
Compras
Batch
Inventarios (MAPICS)
On Line
C x P

5.- ENTREVISTAS CON USUARIOS

5.1. PROBLEMAS REPORTADOS

Entrevistado: Sr. Anselmo Rubio;
Comentarios: No existen problemas actualmente

Entrevistado: Sr. Francisco Godinez
Comentarios: No existen problemas

5.2. PROBLEMAS DETECTADOS

1.- Actualmente se permite capturar materiales y laboratorios que no corresponden entre sí, esta posibilidad de error se puede eliminar validando la relación que existe entre material, laboratorio y división (Jabón, Materias Primas en General), esta actividad la estaba realizando la Lic. Esperanza Sánchez.

RECOMENDACIÓN: Se sugiere terminar esta modificación.

2.- En la captura de maquilas, si no existe la relación material maquilador, envía el mensaje de error correspondiente y al darle entrada al sistema, tiene una salida anormal.

RECOMENDACIÓN: Controlar el resultado de las llamadas a funciones en los programas llamadores.

5.3. MEJORAS SUGERIDAS POR EL USUARIO

El usuario propone que no se le presenten las pantallas que no utiliza cuando es maquila

RECOMENDACIÓN: Si se implementa la recomendación del punto 1, esto se soluciona fácilmente.

6.- REVISIÓN DE LAS INTERFASES

6.1. Diagrama de flujo de datos

Se anexa documento

6.2. Detección de inconsistencias

Se analizaron los programas de actualización de cada módulo y en términos generales estos son correctos; se procedió a revisar el proceso de afectación a las interfases, y una causa de inconsistencias es que se permite efectuar la actualización a las diferentes bases de datos, por dos usuarios concurrentemente, es decir, el modulo adolece de programación multiusuarios.
Se verifico que operativamente es susceptible de ocurrir esta situación, se preparo la comprobación de esta teoría en un ambiente de pruebas.
Se confirmo que efectivamente al hacer la actualización simultánea se afectan erroneamente algunos modulos. En el diagrama de actualización de interfases (anexo), en el paso número seis, si otro usuario ejecuta la misma opción, duplica la afectación de los registros.

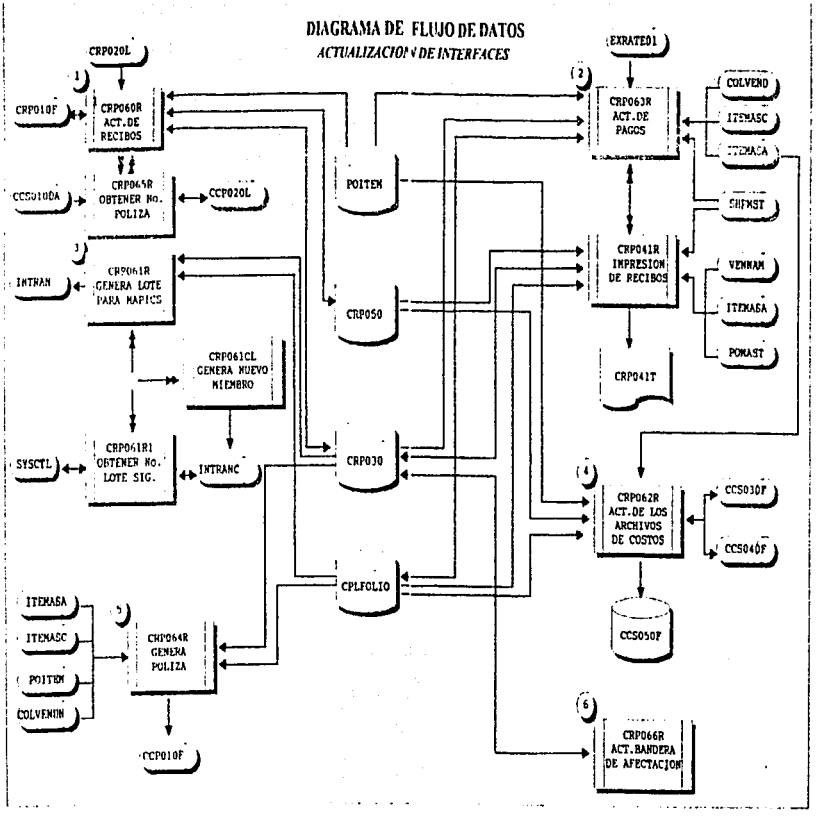


DIAGRAMA DE FLUJO DE DATOS
ACTUALIZACION DE INTERFACES
CRP020L
CRP010F
1
CRP060R ACT.DE RECIBOS
CCS010DA
CRP065R OBTENER No. POLIZA
CCP020L
INTRAN
CRP061R GENERA LOTE PARA RAPICS
CRP061CL GENERA NUEVO MIEMBRO
SYSCTL
CRP061R1 OBTENER No. LOTE SIG.
INTRANC
ITEMASA
ITEMASC
POITEM
COLVENDN
3
CRP064R GENERA POLIZA
CCP010F
POITEM
CRP050
CRP030
CPLFOLIO
EXRATE01
2
CRP063R ACT.DE PAGOS
COLVEND
ITEMASC
ITEMACA
SHFMST
CRP041R IMPRESION DE RECIBOS
VENNAM
ITEMASA
PONAST
CRP041T
4
CRP062R ACT.DE LOS ARCHIVOS DE COSTOS
CCS030F
CCS040F
CCS050F
6
CRP066R ACT.BANDERA DE AFECTACION

7.- ANÁLISIS DETALLADO DE FUNCIONES

7.1. RECEPCIÓN DE MATERIALES
7.2. DEVOLUCIÓN DE MATERIALES
7.3. CANCELACIÓN DE RECEPCIONES
7.4. CONTROL DE CALIDAD
7.5. CONSULTAS
7.6 REPORTES

Como resultado de este análisis se presenta el Plan de Optimización del Modulo.

8.- PLAN DE OPTIMIZACIÓN DEL MODULO

8.1. Relación de problemas

Ver anexo 1.

8.2. Análisis de los problemas

1.- **Falta definir campos de control en la base de datos**, esto ocasiona que para determinar el status de la recepción se utilice: la cantidad de la remisión, el número de la orden de compra, la bandera de actualización de interfases y el folio de control de pagos. Y en base a sus combinaciones se define el status.

2.- **Adolece de programación multiusuarios**. Esto puede causar problemas cómo el demostrado en el punto de afectación de interfases (6.3). Existen otros problemas latentes cómo el cambio y actualización de una misma recepción por dos usuarios, lo que dá resultados no deseados o, también el de las devoluciones debido, a que limpia la bandera de actualización de interfases y manda aplicar el movimiento en sentido inverso, es una fracción de segundo que sí coincide con un llamado de actualización masiva de interfases originada por otro usuario, lo tomaríc como un registro pendiente de actualizar y daría resultados erróneos (no demostrado pero fuera de dudas que pueda ocurrir.)

3.- **No tiene parámetros de control entre programas**. En los llamados entre programas, el llamador no solicita ni recibe mensajes de error, esto causa problemas como el mencionado en el punto 5.2.2.

4.- **Faltan validaciones en los programas de captura.** Esto ocasiona inconsistencia en los datos de la recepción, como el caso de que la fecha de salida fuese más antigua que la fecha de registro, etc. Deben generarse criterios generales de validación para todo el sistema.

5.- **No tiene validación de mensajes de error.** Los programas no incluyen en las rutinas de acceso a la base de datos una validación de los mensajes que regresa el sistema por ejemplo si la lectura/escritura fué o no exitosa y las instrucciones de que hacer en caso de error. Se sugiere se implementen tales instrucciones.

8.3. Sugerencias de Solución

1.- Completar la base de datos con los campos de control y adecuar los programas que resulten impactados por el cambio en la base de datos. Estos campos se pueden agregar al final de los archivos, compilar los mismos con verificación de nivel="no e ir modificando y liberando los programas gradualmente.

2.- Modificar los programas que realizan funciones concurrentes para que trabajen en modo multiusuario, se pueden incluir "data areas" ó código para efectuar este control.

3.- Modificar el control al llamado y retorno de programas, adicionándole un parámetro de respuesta afirmativa o negativa de la tarea efectuada y código para el control de estos errores.

4.- Incluir las validaciones necesarias en los programas de captura de acuerdo con el usuario, debidamente requisitadas en un documento aprobatorio.

5.- Incluir el código y mensajes necesarios para que cualquier error de programa o violación a la integridad de las bases de datos lo notifique el sistema.

6.- Recomendaciones Generales. Se recomienda implantar a la brevedad posible el control de versiones de desarrollo y producción. La capacitación al personal desarrollador debe incluir un pequeño entrenamiento o memorandum para que se habitúen a documentar los cambios en la programación.

RESÚMEN

La programación del módulo (código de RPG, CL y manejo de pantallas) está en un nivel de estructura, segmentación y uso del lenguaje aceptable.
Los errores encontrados no son consistentes, el último fué el de los rechazos de control de calidad, que afectaba algunas interfases erroneámente y, se detectó al cierre de marzo de 19 5.
Los errores de programación para acceso multiusuario y manejo de errores deben corregirse tan pronto como sea posible.

PROPUESTA

Se propone optimizar el sistema de recepción de materiales por fases:

1.- **Corregir las validaciones o adicionarlas a los programas de captura.** Esto permitirá al usuario hacer estrictamente lo que debe hacer. Incluir parámetros para el control de procesos entre programas y monitoreo de la integridad de la base dedatos. Con esto se pretende eliminar el 80% de los problemas presentes y futuros.

2.- **Adecuar la programación a multiusuario**. Incluyendo los controles necesarios para evitar errores por duplicidad de funciones en el mismo momento.

3.- **Completar la base de datos y modificar los programas que resulten impactados por el cambio.** Esto aclarará la programación y le dará mayor estructura para que cualquier persona, es decir, que no sea necesario el conocimiento profundo del módulo para efectuar modificaciones rápidas y exitosas.

4.- **Automatización de procesos.** Eliminar la actualización de interfases por el usuario (F21) y toda liga que tenga con la operación del módulo (cierre de costos, cambio de turno, cierre diario).

ANEXO 1
RELACIÓN DE PROBLEMAS

CRP010R.- Control de la captura de recepción de Materiales
1.- Pérdida del número de almacén.
Solución: Grabar en las notas de recepción el almacén.

2.- Inconsistencia en la validación del laboratorio vs CRP015R.
Solución: Homogeneizar las validaciones.

3.- No muestra el mensaje de error CRP0021.
Solución: Corregir el manejo de pantallas.

4.- Control de status de las recepciones muy complejo.
Solución: Adicionar campos faltantes a la base de datos.

5.- Sin control del resultado de los programas a los que se llama.
Solución: Incluir parámetro de control dentro del área de comunicaciones.

6.- Sin control de programación multiusuarios.
Solución: Incluir el código necesario para efectuar funciones multiusuarios, ya sea controlando el acceso a un laboratorio por usuario o incluir las validaciones pertinentes para que no permita la duplicidad de funciones.

7.- No valida la integridad de la base de datos (ej. que la orden exista en POMAST y POITEM).
Solución: Incluir el código y mensajes necesarios para manejar este error.

8.- No valida el acceso a la base de datos.
Solución: Incluir el código necesario para validar todos los accesos a la base de datos y enviar los mensajes necesarios.

9.- Correcciones sin la documentación necesaria (ej. Bloqueo de instrucciones con asteriscos).
Solución: Documentar correcciones efectuadas. (Autor fecha, causa, solicitante).

10.- Validar opción del subarchivo por progama y quitar de la pantalla.
Solución: Incluir código y mensaje necesario.

CRP011R.- Mantenimiento a recepción de Materiales

1.- Programación compleja, debido a que fué hecho para altas y posteriormente habilitado para cambios.

Solución: Separar las funciones.

2.- Faltan validaciones de la integridad de la base de datos.

Solución: Incluir código necesario para validar los accesos a los diferentes archivos que consulta.

3.- Surtido en exceso, debido a que en el cálculo de la cantidad a recibir no considera recepciones ya actualizadas del día y no afectada en MAPICS, además no verifica que la cantidad recibida sea mayor o igual a cero cuando tiene entregas programadas (error en la actualización a MAPICS).

Solución: Corregir la afectación a MAPICS e incluir recepciones del día en el cálculo y validar la cantidad entregada.

4.- En cambios permite el mantenimiento de movimientos de maquila (5/6) y, según el manual de usuario esto no está permitido, además causaría que se quedarán registros en el CRP020F.

Solución: Bloquear este dato en los cambios para obligar al usuario a cancelar la recepción y darla de alta correctamente.

5.- En caso de retractarse de un cambio el usuario (F3 o F12), restaura la información del CRP010F y nunca la modificó.

Solución: Quitar información de la pantalla (campos ocultos) y eliminar el código que efectúa esa función.

6.- Corregir validación de los datos capturados, cantidad a entregar (acepta cantidades negativas), fecha de llegada (entre el día de hoy y un intervalo de antiguedad), eliminar validación de movimientos de maquila (S,N) de la pantalla y hacerlo por programa con su mensaje respectivo, de los demás datos verificar con el usuario cuando es necesario capturarlo, por ejemplo, si el material es de importación debe exigir la captura del pedimento e investigar cuál sería su validación.

7.- Perdida de números de control, debido a que lo asigna antes de terminar el proceso de captura de la recepción (en el caso de contener entregas programadas y/o movimiento de material en consignación), basicamente lo hace para grabar al CRP010F y con el folio poder accesar está información y no tener que adicionarla en el área de comunicación, aunque esto hace más difícil el entendimiento del programa, poque adiciona y no borra registros a dicho archivo (es decir, lo utiliza como área de comunicación entre programas).

Solución: Incluir el código y mensajes necesarios para manejar este error.

8.- Perdida de números de control, también tiene este efecto cancelar (F3 o F12) la alta o cambio en la pantalla de captura de movimiento de material en consignación, porque borra todo en el CRP010F y deja lo que exista (en el caso de cambios) en el CRP020F (es decir, deja basura).

Solución: Si es cambio, no borrar los registros del CRP010F (dejar como estaban antes del cambio).

9.- Sin controles de programación multiusuarios.

Solución: Incluir el código necesario para poder efectuar funciones multiusuarios.

CRP013R.- Cancelación de recepción de Materiales

1.- Tiene código que no utiliza (ej. key010, key030, rrns) y/o que no efectúa ninguna función (ej. Eliminar registros de archivo de maquilas, no elimina nada; setll a SHPMST y previamente hizo un chain).

Solución: Eliminar código ocioso.

2.- Manejo incorrecto de errores, al llenar un subarchivo valida que la fecha de llegada tenga formato y/m/d, manda el mensaje, pero no efectúa ninguna acción por el error.

Solución: No dejar cancelar la recepción, si existe una violación a los datos, para obligar al usuario a reportarlo a sistemas, se corrija este error y corregir de origen, validando su captura inicial.

3.- Sin controles de programación multiusuarios.

Solución: Incluir el código necesario para poder efectuar funciones multiusuarios.

CRP015R.- Consulta de laboratorios a entregar material.

1.- Tiene código que no utiliza (keyshp).

Solución: Eliminar código ocioso.

2.- Modificar el llenado de subarchivo, hacerlo más eficiente y claro.

Solución: Utilizar posicionamiento (setll) lo cuál hace el acceso a la B.D. más rápido.

3.- No maneja mensaje de error al no seleccionar ningún laboratorio, ni dice como seleccionarlo.

Solución: Incluir el código necesario y mensaje para manejar este error, e incluir la tecla help para informar de cómo se debe seleccionar ó una ventana de los valores permitidos.

CRP016R.- Mantenimiento de notas de recibo de material.
1.- Efectúa funciones innecesarias (ej. Encadena al CRP010F siempre y sólo debe hacerlo si es cambio, si es alta no existe).
Solución: Mover el encadenamiento a donde se hace al CRP040F.

2.- Hace actualización de archivos sin validar su existencia y esto provoca una salida anormal, el programa aborta, fuera de control.
Solución: Incluir código y mensajes para manejar este error.

3.- Corregir validaciones de fecha y hora, debido a que acepta datos erróneos.
Solución: Manejar los rangos adecuados.

CRP025R.- Confirmación de recepción de materiales.
1.-Maneja error de integridad de su base de datos, pero no le avisa al programa llamador ni envía mensaje (si no encadena al registro que va a confirmar da por terminado el proceso).
Solución: Incluir parámetro en el área de comunicación y el código necesario para enviar respuesta y mensaje de error.

2.-Sin control del resultado de los programas a los que llama.
Solución: Incluir parámetro de control dentro del área de comunicación.

3.- Corregir la validación de la fecha de entrada y salida (deben ser mayores o iguales a la fecha de recepción y menores o iguales a la fecha del día, la fecha de entrada debe ser menor o igual que la de la salida y ser fechas validas), e incluir la validación de las horas, anden, número de tarimas, número de camiones.
Solución: Incluir los datos necesarios en el área de comunicación con el CRP040R y eliminar el código.

4.- Sin controles de programación multiusuarios.
Solución: Incluir el código necesario para poder efectuar funciones multiusuario.

5.- Tiene código ocioso (ej. Encadenamiento al CRP010F después de que verifica los folio asignados, y la verificación de los folios tampoco es necesaria, si el programa que los asigna nos manda esta información).
Solución: Incluir los datos necesarios en el área de comunicación con el CRP040R y eliminar el código.

6.-No están bien delimitados los rangos en la asignación de turno.
Solución: Definir exactamente el rango de los turnos.

CRP030R.-Trabajar con distribución de materiales (manejo de entregas programadas).
1.-Inconsistencia en la selección de las partidas vs CRP011R.
Solución: Homogeneizar las validaciones.

2.-No muestra la pantalla de cantidad distribuida (CRP003001).
Solución: Corregir el manejo de pantallas.

3.- Sin controles de programación multiusuarios.
Solución: Incluir el código necesario para poder efectuar funciones multiusuarios.

4.- Incluir documentación en la rutina de proceso de alta (PRCADD), explicando como efectúa el proceso de actualización por cambios y altas. Debido a su interrelación estrecha con el CRP011R.
Solución: Incluir tabla de decisiónes.

CRP040R.- Asigna folio de confirmación del recibo de material.
1.- Corregir texto de la función que efectúa.

2.- Sin controles de programación multiusuarios.
Solución: Incluir el código necesario para poder efectuar funciones multiusuarios.

3.- Sin manejo del resultado de su función.
Solución: Incluir parámetro de respuesta dentro del área de comunicación y el código necesario para enviarla.

4.- Maneja error de la integridad de su base de datos, pero no le avisa al programa llamador ni envía mensaje.
Solución: Incluir el código necesario y mensaje para manejar el resultado de la llamada.

5.- Compleja la determinación del status apropiado para asignarle el folio.
Solución: Completar la base de datos con campos de control y modificar el código que resulte afectado.

CRP050R.- Mantenimiento de material en consignación.

1.- Corregir validación de datos a capturar:

a) Si no registran tipo de movimiento no envía mensaje, no valida los datos capturados y así, graba el registro aún sin datos.

b) Si son varios registros y el último no tiene error, aunque todos los anteriores sean erróneos, así los graba y no envía mensajes de error.

c) No valida la relación entre material en consignación (MATCO) y el número de parte (ITNBR). En el caso de recepciones la validación se debe efectuar con el CCS120F, para envíos deben ser iguales.

d) No valida la cantidad. Si se valida la relación mencionada en el punto anterior, para recepciones el programa debería calcularla y en envíos la suma de las cantidades a enviar debe ser igual a la del movimiento.

Solución: Modificar e incluir el código necesario para efectuar las validaciones correctamente y, completar las relaciones en el archivo CCS120F.

2.- Faltan validaciones de la integridad de la base de datos.

Solución: Incluir el código necesario para validar los accesos a los diferentes archivos que consulta y el envío de mensajes (ITEMASA, VENNAM, CRP010F.)

3.- Corregir respuesta del resultado de su proceso, cuando no graba ningún registro de maquila de todos modos manda una respuesta afirmativa.

Solución: Obligar a que capturen algún registro o cancelen el proceso.

CRP070R.- Proceso de devolución de materiales.

1.- Sin control del resultado de los programas a los que llama.

Solución: Incluir parámetro de control dentro del área de comunicación.

2.- Inconsistencia en la validación del laboratorio vs. CRP015R.

Solución: Homogeneizar las validaciones.

3.- Faltan validaciones de la integridad de la base de datos.

Solución: Incluir el código necesario para validar los accesos a los diferentes archivos que consulta y el envío de mensajes (ITEMASA, VENNAM.)

4.- Codificar de manera explícita la verificación de si ya fué facturada la recepción de material, en la subrutina de rellenado del subarchivo (FILSFL.)

Solución: Validar que exista la recepción den CPLFOLIO y no tener número de factura.

CRP090R.- Calificación de control de calidad.
1.- Inconsistencia en la validación del laboratorio vs. CRP015R.
Solución: Homogeneizar las validaciones.

2.- Control de proceso muy complejo, debido a que tiene código ocioso y mezcla de funciones.
Solución:Eliminar código ocioso, definir correctamente las funciones y ajustar el código a esas funciones.

3.- Efectúa proceso de validación de la segunda pantalla antes de verificar que los datos registrados en la primera (CRP09001) sean correctos.
Solución: Corregir código para que valide correctamente.

4.- Faltan validaciones de la integridad de la base de datos.
Solución: Incluir el código necesario para validar los accesos a los diferentes archivos que consulta y el envío de mensajes (ITEMASA, VENNAM.)

5.- Sin controles de programación multiusuarios.
Solución: Incluir el código necesario para efectuar funciones multiusuarios.

6.- Sin control del resultado de los programas a los que llama.
Solución: Incluir el parámetro de control dentro del área de comunicación.

7.- Eliminar el cambio de dato registrado en pantalla cuando el folio solicitado está pendiente por calificar (MSGID=CRP0039). Debido a que crea confusión en la presentación de los datos (si se da otro intro), ver anexo, o sí hace el cambio que le efectúe completo.
Solución: Eliminar el cambio de dato.

8.- Incluir en la pantalla (CRP09004) el dato de la fecha o el laboratorio del cuál no existen registros a presentar.
Solución:Incluir el código necesario para efectuar este cambio.

9.- Validar opción de subarchivo por programa y eliminar de la pantalla, validando que si es proceso de pendientes sólo es valida la opción 1 (si es valida la opción 2 hacerlo explícito) y, si es por histórico son validas ambas.
Solución: Incluir código y mensaje necesario.

BIBLIOGRAFIA

Bell, Judy Kay, Disaster Survival Planning: A Practical Guide for Business, USA, 1991.

Brown, W.S. Auditing with the Computer, Berkeley, Calif., University of California Press, 1975.

Colegio de Contadores Públicos de México, Diferentes Enfoques de Auditoría en Informática, México, mimeo, 1991.

Colegio de Licenciados en Ciencias Políticas y Administración Pública, A.C., Diccionario de Política y Administración Pública, coordinado por Mario Martínez Silva, México.

Chiavenato, Adalberto, Introducción a la Teoría General de la Administración Pública, México, Ed McGraw Hill, 1984.

Davis, Gordon Bitter, La Auditoría y el Procesamiento Electrónico de Información, México, Instituto Mexicano de Contadores Públicos, A.C., 1972.

Franco Romo, Alfonso, et. al., Planeación de la Recuperación Informática en caso de Desastre, Facultad de Contaduría y Administración, México, UNAM, mimeo, 1990.

Higley Russell, Susan; Eason Tom, S.; Fitzgerald, J. M., Data Processing Control Practices Report, The Institute of Internal Auditors, Inc. Standfor Research Institute, USA, 1989.

Historia de la Asociación Mexicana de Auditores en Informática, A.C., México, AMAI, 1985.

I.B.M., The Auditor Encounters Electronic Data Processing. Nueva York, Price Waterhouse and Co. e International Business Machines Corp., 1956.

Lambarri Valencia, Alejandro, Curso de Auditoría Informática, México, mimeo.

Lawrence, Charles, Procedimientos de Auditoría, 2ª ed., México, Ed. Herrero.

Lazcano, Juan Manuel y Rivas Zyvy, Enrique, Auditoría en Informática. Estructuras en Evolución; México, Instituto Mexicano de Contadores Públicos A.C., 1988.

López Elizondo, La Profesión Contable. Selección y Desarrollo, 3ª ed., México, Ed. ECASA, 1984.

Mair, William C.; Wood, Donald R., et. al., Computer Control & Audit, The Institute of Internal Auditors, USA, 1978.

Mathelot, Pierre, L'Informatique, que sais-je, France, Presses Universitaires de France, 1980.

Myers, Kenneth N., Total Contingency Planning for Disasters, USA, 1993.

Nelson, John R., Auditing in a Microcomputer Environment; Instructor's Guide, Florida, Institute of Internal Auditors, 1980.

Price Waterhouse and Company, Use of Computers in Auditing: a Professional Development Course in Electronic Data Processing, New York, 1987.

Porter, W. Thomas, Jr., Auditoría de Sistemas Electrónicos, 2ª ed., México, Ed. Herrero, 1971.

Ramírez Bustos, Juan y Valdez Hernández, Alfredo, Desarrollo Tecnológico, una Posibilidad al Alcance de su Empresa, México, FONEI, 1982.

Real Academia Española, Diccionario de la Lengua Española, España, Ed. Espasa-Calpe, 1992.

Sanders H., Donal, Informática: Presente y Futuro, México, Ed. McGraw Hill, 1985.

Slosse, Carlos, et al., Auditoría, Un Nuevo Enfoque Empresarial, 2ª ed., Buenos Aires, Argentina, Ediciones Macchi.

Tradeway Commission, Reporte Final 1992, Coautoría / COSO, 1992.

United States Air Force, Department of, Guide for Auditing Automatic Data Processing Systems, Washington, D.C.: Government Printing Office, 1961.

Weber, Ron, EDP Auditing, Conceptual Foundations and Practice, 2ª ed., USA, McGraw Hill, 1988.