33
2eje.

UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ACATLAN

AUDITORIA A LOS SISTEMAS DE INFORMACION COMPUTARIZADAS EN OPERACION

T E S I S

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN MATEMATICAS APLICADAS Y COMPUTACION

P R E S E N T A :

SERGIO ALFONSO TRONCOSO PEREZ

ACATLAN, EDO. DE MEXICO 1994

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

VNIVERSIDAD NACIONAL AVENTMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES "ACATLAN"

DIVISION DE MATEMATICAS E INGENIERIA
PROGRAMA DE ACTUARIA Y M.A.C.

SR. SERGIO ALFONSO TRONCOSO PEREZ
Alumno de la carrera de M.A.C.
P r e s e n t e .

Por acuerdo a su solicitud presentada con fecha 28 de abril de 1993, me complace notificarle que esta Jefatura tuvo a bien asignarle el siguiente tema de Tesis: AUDITORIA A LOS SISTEMAS DE INFORMACION COMPUTARIZADOS EN OPERACION", el cual se desarrollará como sigue:

INTRODUCCION
CAP. I Conceptos de Sistemas de Información.
CAP. II Auditoría en Informática.
CAP. III Controles a los Sistemas de Información.
CAP. IV Metodología para evaluar un Sistema de Información Computarizado en Operación.
CAP. V Aplicación de un caso Práctico.
CONCLUSION.
GLOSARIO.
APENDICE.
BIBLIOGRAFIA.

Asimismo, fué designado como Asesor de Tesis el ING. PABLO HECTOR GONZALEZ VIDEGARAY, Profesor de esta Escuela.

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

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Acatlán, Edo. Méx. Noviembre 14 de 1994.

ACT. LAURA MA. RIVERA BECERRA
Jefe del Programa de Actuaría
y M.A.C.

cg'

A DIOS

"Verdaderamente Dios ha oido, a prestado a la voz de mi oración"

Salmos 66 : 19

Gracias por no olvidarte de mi y permitirme lograr un objetivo más.

A MI FAMILIA

Con todo mi amor a mis padres, DAVID y MARIA ANGELES, que sin su apoyo, esmero y dedicación con migo no hubiera sido posible este logro.

A mis hermanos, David, Laura y Jorge.

A mi cuñado y sobrinos, Henrique, Henrique Jr. y Bárbara.

A MIS AMIGOS

Por su cariño, apoyo, comprensión y amistad, tanto en el estudio como en el trabajo.

AGRADECIMIENTOS

A mis profesores y compañeros que durante mi estancia en la carrera me brindaron lo mejor de si mismos.

INDICE

TEMA: " AUDITORIA EN INFORMATICA "

TITULO: " AUDITORIA A LOS SISTEMAS DE INFORMACION COMPUTARIZADOS EN OPERACION "

INDICE

INDICE

INDICE

INDICE

INDICE

INDICE

INDICE

INTRODUCCION

Objetivo

Al realizar esta investigación, se describe cómo es conducida la Auditoria en Informática, aplicando una metodología estandarizada para evaluar el grado de confiabilidad e integridad de los datos en un sistema de información computarizado en operación de un área organizacional, de igual forma, comprender los beneficios de la Auditoría Informática.

La auditoría informática es la recolección y evaluación de evidencia, para determinar si un sistema automatizado : salvaguarda activos, mantiene la integridad de los datos, alcanza las metas organizacionales y consume recursos eficientemente. La salvaguarda de activos, se refiere a garantizar que se encuentran protegidos de daños o destrucción, uso no autorizado o robo. La integridad de los datos es un estado, que significa que la información sea precisa, completa y consistente. Ambas, la salvaguarda de activos y la integridad de los datos, son importantes para los auditores en informática, también, considera una inquietud por efectividad con la cual los sistemas de información logran sus objetivos y la eficiencia con que la información es procesada.

Debido a que los Sistemas de Información han llegado a ser un elemento considerable, generador de gastos para una compañía, la gerencia pide con más frecuencia a los auditores informáticos la evaluación de estos aspectos en dichos sistemas.

Justificación del tema

A causa de que las computadoras son utilizadas más intensamente en el procesamiento de información; con el advenimiento de hardware y software más sofisticado, es necesario contar con los procedimientos y controles adecuados para que los sistemas de información computarizados en operación mantengan el nivel de confiabilidad y eficiencia para que cumplan con los objetivos organizacionales.

Hipótesis

Al concluir el trabajo de tesis comprobare que la metodología estandarizada propuesta es util y eficiente al evaluar los sistemas de información.

Resumen del capitulado

La tesis se encuentra dividido en cinco capítulos :

El capítulo uno son conceptos de Sistemas de Información, trata lo concerniente a definiciones de sistemas de información, su clasificación y el nivel de auditoría de cada sistema, definiendo la función del auditor interno y externo al analizar y evaluar los sistemas.

El capítulo dos es Auditoría en Informática, trata los antecedentes de la auditoría en informática, así como las definiciones de auditoría, auditoría financiera y auditoría en informática. Describe las funciones de la auditoría informática para una óptima administración de sus actividades, y por último describe las normas generales y el código de ética las cuales rigen las actividades del auditor al evaluar los sistemas de información computarizados.

El capítulo tres trata los Puntos de Control al operar los Sistemas de Información y su clasificación, los cuales son : controles de entrada, de proceso, de programas de aplicación, de base de datos, de operación de la computadora, de biblioteca, de seguridad y de salida, principalmente.

El capítulo cuatro expone una metodología estandarizada para evaluar un Sistema de Información Computarizado en Operación, explicando cada uno de los pasos a seguir para realizar una auditoría a un sistema en específico.

El capítulo cinco y último expone un caso práctico aplicando los procedimientos y controles en la auditoría informática descritos en los capítulos anteriores, se evaluará un sistema de información específico : un sistemas de Cuentas por Cobrar de una Empresa Manufacturera, la auditoría cubre desde la planeación estratégica hasta la emisión de los resultados de la auditoría.

CAPITULO I

INTRODUCCION

Los avances en la tecnología de computación a menudo marchan paralelos a los avances en los negocios. Los sistemas distribuidos de procesamiento de datos fueron desarrollados para ayudar a la Directivos a colectar y organizar información, dentro de una organización ampliamente dispersa. Los sistemas distribuidos han ayudado a muchas compañías a expander sus negocios , ofrecer a sus clientes muchos servicios nuevos y monitorear la información producida por estas actividades. La computadora es vital para estas operaciones distribuidas por su capacidad para procesar la información que entra a una compañía y dar a los gerentes los datos necesarios para administrar. Los gerentes de otras áreas en las compañías recurren constantemente al personal de sistemas por la información operativa, vital para una administración activa y exitosa.

En este cápitulo doy definiciones de sistemas de información, y su clasificación, de igual forma, trato las definiciones de los Sistemas de Información Gerencial "SIG", su estructura y funcionalidad dentro de una organización; finalmente describo la función del auditor en informática externo e interno en la unidad de negocio.

Por tanto, asi como no hay dos compañías que funcionen de la misma manera, la mayoría de los servicios de procesamiento de datos también son únicos.

1. CONCEPTOS DE SISTEMAS DE INFORMACION

1.1. Definición de Sistemas de Información

Un sistema es un grupo de partes integradas que tienen el propósito común de lograr algún o algunos objetivos, el sistema está conformado por:

1. Grupo de partes: Un sistema tiene más de un elemento. Una bola de acero no es un sistema, pero podría formar parte de una norma de cojinetes que pueden ser combinados con otros componentes para producir un sistema de riego.

2. Partes integradas: Debe existir una relación lógica entre las partes de un sistema. Los sistemas electrónicos, como los juegos de video, tienen componentes que trabajan juntos.

3. Propósitos comunes para el logro de algun (os) objetivo (os). El sistema es diseñado para cumplir uno o más objetivos.

Todos los elementos de un sistema deben ser controlados de tal modo que la meta del sistema sea alcanzada. Los sistemas automatizados tienen sus operaciones estrechamente controladas.

La computadora es un conjunto de partes integradas que tienen el propósito común de realizar las operaciones necesarias para ejecutar el programa; también es un sistema.

Ahora bien, cualquier sistema puede ser compuesto de pequeños sistemas o subsistemas. Un subsistema es un sistema pequeño incluido en uno más grande.

Algunas de las partes componentes encontradas en la mayoría de los sistemas de computadora; y las computadoras, a su vez, pueden ser consideradas subsistemas de otros sistemas, tales como el control de tráfico aéreo usado para vigilar el vuelo de las aeronaves de un país.

De igual forma, una orgnización de negocios, es un sistema compuesto por muchas actividades o componentes (subsistemas). Cada uno de estos componentes interactúa con otros componentes, para contribuir a la realización de metas planeadas previamente.

Por lo anterior, el concepto de sistemas hace hincapié:

1) En las relaciones entre los subsistemas, y

2) En la influencia que tienen esas relaciones en el comportamiento y la actuación de otros subsistemas.

Debemos ocuparnos de la organización y de las operaciones de procesamiento de datos, tanto manuales como relacionadas con las máquinas, a fin de producir información sobre un proyecto determinado, en forma deseada y con un costo mínimo.

Si consideramos a una empresa comercial como un sistema, cada uno de los siete circulos internos mostrados en la figura 1.1. constituye un sistema que a su vez crea información para ayudar al funcionamiento de los otros seis subsistemas, mientras que continúa con sus funciones internas, y éstos a su vez, interactuan con las funciones del sistema de nóminas.

LA ORGANIZACION COMO SISTEMA

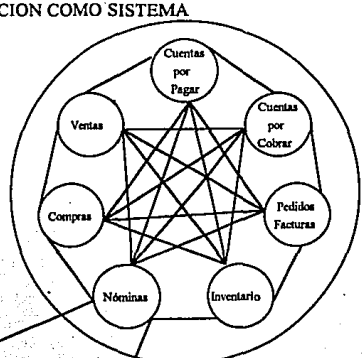


Figura 1.1.

LA NOMINA COMO SISTEMA

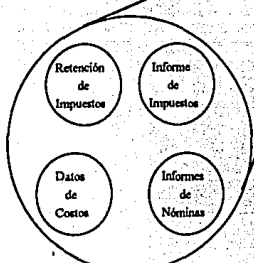


Figura 1.1. - A

Una organización como sistema se compone de subsistemas generadores de información.

Por ejemplo, aunque el departamento de nóminas es un subsistema (componente) de una organización, contiene un sistema completo de información, en términos de las diversas operaciones que debe ejecutar para producir los datos de la nómina, figura 1.1-A. En esta actividad está implícito el hecho de que cada subsistema tiene su propio objetivo, mientras que lo que hace, contribuye al logro de los importantes objetivos de la organización.

Hay que tomar en cuenta que para que un sistema de información funcione eficazmente, ningún subsistema puede trabajar independientemente de los demás, sino que debe trabajar en armonía con ellos.

1.2. CLASIFICACION DE LOS SISTEMAS DE INFORMACION

Los sistemas según su diseño pueden ser de tipo conceptual o empírico y ubicarse en alguna de las siguientes áreas:

1. Conceptual, si se discute la teoría de la organización

2. Empírico, si se discuten las personas y sus relaciones reales.

3. Natural, si se discuten las personas como parte de la ecología de la vida sobre la tierra.

4. Manufacturado, si nosotros discutimos cualquiera otro tipo de actividad humana.

5. Social, toda organización humana que sea sujeta a ser considerda para investigación.

6. Abiertos, todas las organizaciones sociales son sistemas abiertos porque su reaccion es interrelacionada con el medio ambiente.

7. Permanente, se pueden considerar sistemsa políticos y compañías muy antiguas como tipo de sistema permanente, en otros casos se consideran temporales.

8. No estacionarios, los sistemas organizacionales tienden a adaptarse al cambio del medio ambiente.

Para casos de estudio es mejor tratar a los sistemas como estacionarios.

9. Subsistemas y suprasistemas, varían dependiendo de su ubicación.

10. Adaptativo, es una modalidad de los sistemas organizacionales, que consiste en que toda organización se adecúa al medio ambiente que le rodea para su funcionamiento.

1.3. ELEMENTOS DE LOS SISTEMAS DE INFORMACION

Los componentes del sistema (subsistema y elementos de éstos) contienen objetos, personas, posesión de propiedades o características, donde estas características afectan la operación de los sistemas en velocidad, en precisión, confiabilidad, capacidad, etc.

La estructura de un sistema es el conjunto de relaciones entre objetos y atributos; los niveles de relaciones pueden ser clasificados como:

De primer orden: Relaciones funcionales y disfuncionales causada por fenómenos naturales o variación de los atributos.

De segundo orden: Simbiosis, la relación necesaria entre organismos disimilares.

De tercer orden: Relación sinergética en la cuál los atributos de los objetos se refuerzan unos a otros para incrementar o reforzar los sistemas de salida.

El procesamiento total de un sistema es el resultado neto de todas las actividades convertidas de entradas en salidas. La relación funcional entre la entrada y la salida de un proceso es llamado "Función de Transferencia". Este término es comunmente usado en el diseño y evaluación de sistemas de retroalimentación.

El concepto de límites de un sistema hace posible enfocarlo sobre un sistema en particular sin una jerarquía de sistemas. Los límites de un sistema pueden ser tanto físicos como conceptuales.

La definición operacional de un sistema de información en términos de sus límites es :

1. Listar todos los componentes del sistema y aquellos que lo circunscriben.

2. Listar todos los flujos a través de sus límites. Los flujos del medio ambiente hacia el sistema y el flujo de sus salidas hacia sus límites.

3. Identificar todos los elementos que contribuyen al objetivo específico del sistema, incluyendo sus límites.

El conocimiento y análisis de las caraterísticas de los sistemas es de suma importancia para el diseño, producción, diagnóstico y evaluación del mismo.

1.4. SISTEMAS DE INFORMACION GERENCIAL (SIG)

Los sistemas distribuidos de procesamiento de datos fueron desarrollados para ayudar a los Directores a colectar y organizar información, dentro de una empresa. Los sistemas distribuidos han ayudado a muchas compañías a expander sus negocios, y a monitorear la información producida por estas actividades. La computadora es vital para estas operaciones distribuidas por su capacidad para procesar la información que entra a la compañía y dar a los Gerentes los datos necesarios para administrar.

A los sistemas de información operacional se les conoce como sistemas de información gerencial, proporcionan a los gerentes información necesaria para dirigir una organización y para tomar decisiones.

Los SIG se diseñaron para producir la misma información que los puntos relevantes de las condiciones a las cuales debe reaccionar la gerencia. Los sistemas de información gerencial están soportados por sistemas de computo bastante grandes. Esta amplia capacidad de proceso es desperdiciada cuando los empleados proporcionan información equivocada o incompleta, los usuarios no entrenados para usar los dispositivos periféricos anulan completamente el efecto del "SIG".

El personal, las máquinas y la computadora deben estar organizadas para producir los resultados deseados : información que pueda usar la gerencia en la toma de decisiones.

1.4.1. Características de la Información Gerencial

Como regla general, entre más sirva una información para reducir la incertidumbre de las decisiones efectuadas por los directivos en todos los niveles, mayor será su valor.

El costo de la información obtenida debe compararse con los beneficios obtenidos para su uso. La información exacta, oportuna, íntegra y concisa tiene más valor que la que carece de una o varias de éstas características; sin embargo, con frecuencia se sacrifica alguna de ellas por razones económicas.

EXACTITUD. La exactitud es el porcentaje de información correcta respecto al total de información generada en un periodo.

Si son generadas 1000 unidades de información y 950 de ellas dan un reflejo fiel de la situación, entonces el nivel de exactitud es de 0.95%; que éste nivel sea lo suficientemente alto depende de la información generada.

OPORTUNIDAD. La oportunidad es otra característica importante de la información. El tiempo de respuesta debe ser lo suficientemente breve para que tenga poco volumen, bajo costo y descubra las tendencias importantes que señalen la necesidad de una acción.

Cuando se requiera el acceso inmediato a la información, con alta sensibilidad al factor tiempo, se debe utilizar la rápida respuesta de los sistemas en línea.

INTEGRIDAD. La mayoría de los directivos se han enfrentado alguna vez con la necesidad de tomar una decisión y se han encontrado de que la información es exacta, oportuna pero incompleta. Una mejor integración de los hechos disponibles, diseminados en una empresa, con el objeto de proporcionar a los directivos información más completa, es la meta de los diseñadores de los sistemas de información.

CONCISION. Muchos sistemas tradicionales de información han sido proyectados con base a la premisa en el problema más grave que enfrentan los directivos en la falta de información completa.

La información concisa que resumen los datos importantes y señalan las áreas de excepción de las actividades normales o planeadas, es lo que con mayor frecuencia necesitan los directivos, pero también es lo que menos se les proporciona.

El concepto del "SIG" ha sido definido de diversas formas. Ya que el modelo "SIG" de una organización difiere del de otra.

1.4.2. Definición del SIG

Los sistemas de información gerencial "SIG" son un conjunto de procesos de datos en computadoras, proyectados e implementados en una organización e integrados con procedimientos manuales y de otro tipo, cuyo propósito es proporcionar información eficáz y oportuna para apoyar la toma de decisiones y otras funciones de la gerencia.

Los modelos "SIG" difieren, la mayoría reconoce los conceptos que se muestran en las figuras. Además de lo que podría llamarse estructura horizontal gerencial como se muestra en la figura 1.2-A; así también, una organizacion se divide en distintas especialidades y funciones empresariales que requieren flujos separados de información como se muestra en la figura 1.2-B. La figura 1.2.-A esta formada por la alta gerencia quien se encarga de la toma de disiciones, la gerencia media pone en marcha el plan de trabajo a desarrollar y finalmente la gerencia operativa se encarga de realizar el trabajo. La figura 1.2.-B muestra los diferentes departamentos de una organización ejemplificados de forma vertical.

Figura 1.2. - A

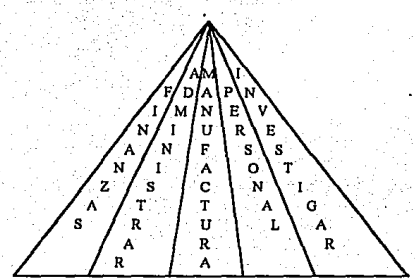


Figura 1.2. - B

Al combinar los niveles gerenciales horizontales con las especialidades (departamentos) empresariales verticales, se forma la compleja estructura de organización que se muestra en la figura 1.2-C, las cuales utilizan una base de datos en sus operaciones diarias.

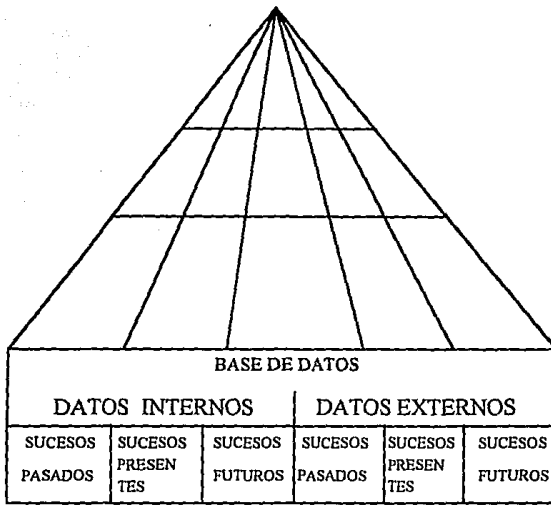


Figura 1.2. - C

Esta estructura es fundamentalmente una base de datos constituida por datos generados interna y externamente, relativos al pasado, al presente y a pronósticos de sucesos futuros.

1.4.3. Aspectos Organizacionales y el SIG

La función de organización comprende la agrupación de personas y otros recursos en unidades lógicas y eficientes para llevar a cabo planes y lograr objetivos. Al diseñar e implantar el "SIG" existe la necesidad de reconsiderar las respuestas a diversas interrogantes importantes e interrelacionadas acerca de la organización :

* ¿Se centralizará o desentralizará la toma de decisiones?

* ¿El procesamiento de datos estará concentrado o disperso?

* ¿Se almacenarán los datos en forma concentrada o dispersa?

* ¿Dónde se localizarán los recursos computacionales?

* ¿Cómo se organizará la función del "SIG"?

1.4.4. Organización del Departamento SIG

La organización del departamento SIG puede adoptar diversas formas.

La función del administrador de bases de datos, se ubica en un departamento "SIG" y sus actividades incluyen el establecimiento y control de la definición de los datos, la definición de las relaciones entre los datos, y el diseño del sistema de seguridad de la base de datos para prevenir el uso no autorizado. La sección de análisis / diseño del sistema es la interfase esencial entre los grupos de usuarios y las otras secciones del departamento "SIG".

La función de preparación de programas se subdivide en nuevos grupos de aplicaciones y mantenimiento, y la función de la sección operaciones de la computadora es preparar los datos de entrada y producir información de salida continuamente, el control del tiempo de la computadora y la programación de actividades de procesamiento son obligaciones del supervisor de operación. También son necesarios los controles para asegurar que los datos de entrada sean correctos. Los operadores de los dispositivos de entrada y los bibliotecarios trabajan en esta sección. La función de telecomunicaciones también puede ubicarse en cualquier parte, existe creciente tendencia a asignar a un solo ejecutivo de administración de información.

Las responsabilidades de los servicios de cómputo y las telecomunicaciones, la investigación de operaciones es la metodología cuantitativa y el conocimiento que se emplean para apoyar a los directivos en la toma de decisiones.

Quienes están en la seccion de investigación de operaciones pueden dedicarse a otros aspectos de la planeación de la empresa, pero se requiere el uso de computadoras y base de datos para respaldar los sistemas de apoyo de la planeación y las decisiones que el personal de investigación de operaciones ayuda a proyectar. Por esto es posible incluirlos en un departamento "SIG" como se muestra en la figura 1.3.

Organización funcional del departamento SIG.

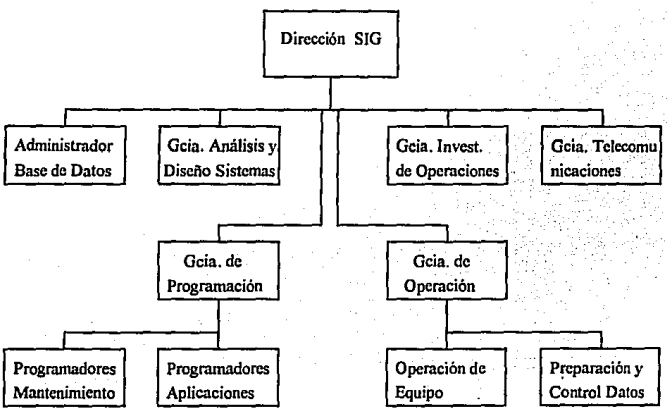


Figura 1.3.

1.5. LA FUNCION DEL AUDITOR INTERNO Y / O EXTERNO EN INFORMATICA DENTRO DE LAS ORGANIZACIONES.

Después del elemento humano, el recurso más valioso para cualquier empresa es sin duda el de la información. Los equipos y sistemas de cómputo ayudan a incrementar ese valor al mejorar su oportunidad, confiabilidad, uso y almacenamiento.

La revolución tecnológica ha transformado las estructuras mecánicas operativas hasta un punto tal que la información, ha alcanzado para fines de servicio un valor semenjante al del dinero.

Sin embargo, es necesario tener un concepto claro de este importante activo de las empresas, ya que dependiendo del uso que se le dé, puede alcanzar altos niveles de utilidad, o por el contrario perder cualquier margen de oportunidad.

La información es un conjunto de datos procesados o integrados dentro de un contexto, de manera que reducen la incertidumbre.

Es la materia prima para el proceso de clarificación de situaciones y hace que la decisión correcta sea más facilmente identificable.

Durante el proceso normal de la información, puede llegar un momento en que el volumen es tal, que manejarla en forma manual desde su recopilación y análisis hasta su síntesis, sería demasiado tardado, y aquí es en donde resulta útil el computador.

Este elemento tecnológico se convierte en un factor estratégico dentro de cualquier organización por su capacidad de almacenar y procesar grandes volúmenes de información, pero tal vez se identifican riesgos, peligros y retos al compartir, transmitir y proteger la información corporativa.

Desde este punto de vista se debe considerar la función del Auditor en Sistemas de Información (ASI , siglas que utilizaremos en el transcurso del trabajo para referirnos al auditor), como un experto en diferentes aspectos, desde la operación de sistemas de información complejos, hasta el conocimiento detallado de los esquemas de seguridad física y lógica en los diferentes ambientes del procesamiento electrónico de datos.

Aprovechando la alta tecnología en materia de procesamiento electrónico y comunicaciones, el auditor en informática debe reorientar la forma de revisar los controles internos ahora aplicados a los sistemas automatizados.

Es así como el ASI comienza la evaluación de eventos y clasificación de resultados pudiendo facilitar y agilizar el diseño y control de los mecanismos que reportan la efectividad de las normas y lineamientos en el sistema.

Lo que debe de esperarse de un grupo de Auditoria en Informática es asegurar y persuadir a los grupos desarrolladores y usuarios finales, de la necesidad y beneficios de la aplicación de políticas de sistemas de prueba para el desarrollo de nuevos sistemas o cambios a los existentes.

Independientemente de la capacidad y habilidad del ASI, no se puede estar sujeto a una tradicional recolección de información y las pruebas de verificación. Estos principios consideran a la documentación, seguimiento y controles diseñados para la construcción de tales sistemas.

CAPITULO II

INTRODUCCION

La auditoria en Informática es el proceso de recolección y evaluación de evidencia para determinar si los sistemas computacionales : salvaguardan activos, mantienen la integridad de los datos y alcanzan las metas de una organización efectiva y eficientemente.

La salvaguarda de activos se refiere a asegurar que se encuentran protegidos de daños, o destrucción, uso no autorizado o bien de robo. La integridad de datos es un estado, que significa que la información sea precisa, completa y consistente. Ambas, la salvaguarda de activos y la integridad de datos han sido siempre de interés para los auditores. Sin embargo, la definición de auditoria en informática propuesta, también considera una inquietud por efectividad con la cual los sistemas de información logran sus objetivos, y la eficiencia con que la información es procesada. Debido a que el área de informática ha llegado a ser un elemento considerable, generador de gastos para una compañía, la gerencia pide con más frecuencia a los auditores la evaluación de estos aspectos a los sistemas computacionales.

Como hemos visto la auditoria en informática es una actividad profesional que se desarrolló para asegurar que los sistemas computacionales en efecto, salvaguarden activos, mantienen la integridad de los datos y alcancen las metas de una organización efectiva y eficientemente. La gerencia de las compañías, debe estar interesada en saber si sus sistemas computacionales cumplen con estos objetivos.

Hace treinta años las necesidades de procesamiento de datos se satisfacían manualmente; hoy en dia las computadoras realizan gran parte del procesamiento de datos.

La necesidad de mantener la integridad de los datos procesados por las computadoras prevalece en nuestras vidas. Actualmente existe un gran temor de que las substancialmente incrementadas capacidades de procesamiento de datos no sean adecuadamente controladas, ya que se pueden realizar delitos por computadora.

El uso incontrolado de computadoras ha extendido un impacto general en la sociedad. Los fraudes son perpetrados debido a controles inadecuados a los sistemas. De este modo la auditoría en informática soporta el logro de los objetivos de auditoría tradicionales : objetivos de certificación (para auditores externos) que hacen énfasis en la salvaguarda de activos e integridad de datos y objetivos gerenciales, (para un auditor interno) que se enfoca no sólo a objetivos de certificación pero también a objetivos de efectividad y eficiencia. El proceso de auditoría en informática se puede concebir como la fuerza que ayuda a las organizaciones a lograr mejor estos objetivos.

2. AUDITORIA EN INFORMATICA

2.1. ANTECEDENTES DE LA AUDITORIA EN INFORMATICA

Los más claros antecedentes del inicio de la auditoría en informática los encontramos en Estados Unidos con la fundación de la Asociación de Auditores de Procesamiento de Datos ((EDPAA) The .Electronics Data Processing Auditing Association) en el año de 1969, teniendo como objetivos básicos, fomentar la educación, comunicación, el desarrollo profesional e investigación en los campos relacionados con la auditoría y sistemas de información.

Para el año de 1976 fue organizada la Fundación de Auditores de Procesamiento Electrónico de Datos (The Electronic Data Processing Auditors Foundation (EDPAF)) como ente no lucrativo y dedicado a fomentar la educación, comunicación, desarrollo profesional, elaboración de normas e investigación con lo relacionado a los campos de Auditoría en Sistemas de Información.

Posteriormente el 21 de junio de 1978, la Fundación de Auditores de Procesamiento Electrónico de Datos anuncia oficialmente un programa de Certificación Internacional de manera anual (CISA (Certification Information System Auditors)), de la Asociación de Auditores de Procesamiento Electrónico de Datos.

Los objetivos formales fueron :

* Desarrollar y mantener un instrumento de verificación que evalúe la competitividad de un individuo en la conducción y auditoría de sistemas de información.

* Proporcionar un mecanismo para motivar a los auditores en sistemas de información, a mantener su competitividad y monitorear los logros en los programas de mantenimiento.

* Ayudar a la Alta Dirección para desarrollar una función de auditoría en sistemas de información, ofreciendo criterios para la selección y desarrollo profesional.

Finalmente surge en nuestro país la Asociación Mexicana de Auditores en Informática (AMAI), con la finalidad de difundir los avances tecnológicos en esta área con objeto de lograr así la actualización profesional continua.

2.2. AUDITORIA A SISTEMAS DE INFORMACION COMPUTARIZADOS

La auditoría es un proceso dentro de toda organización que por siempre se ha desarrollado de una manera intrinseca en cada actividad de ésta, es solo hasta las epocas recientes que se ha establecido cómo función dentro de la estructura organizativa, esto devido a las complejas actividades que han de supervisarse y las múltiples transacciones realizadas.

2.3. DEFINICION DE AUDITORIA EN INFORMATICA

La auditoría en informática es el proceso de recolección y evaluación de evidencia, para determinar si un sistema automatizado: salvaguarda activos, mantiene la integridad de los datos, alcanza las metas organizacionales efectivamente y consume recursos eficientemente.

La salvaguarda de activos, se refiere a garantizar que se encuentran protegidos de daños o destrucción, uso no autorizado o bien de robo. La integridad de datos es un estado, que significa que la información sea precisa, completa y consistente. Ambas, la salvaguarda de activos y la integridad de los datos, han sido siempre de interés para los auditores. Sin embargo, la definición de auditoria en informática propuesta, también considera una inquietud por la efectividad, con la cual los sistemas de procesamiento electrónico de información logran sus objetivos y la eficiencia con que la información es procesada.

Debido a que el procesamiento electrónico de información ha llegado a ser un elemento importante, generador de gastos para una compañía, la gerencia pide con más frecuencia a los auditores la evaluación de éstos aspectos a los sistemas de información computarizados.

En las decádas de los años 60's y los años 70's, la mayoria de las necesidades de procesamiento de datos se satisfacían manualmente; hoy en día las computadoras realizan gran parte del procesamiento de datos requerido. La necesidad de mantener la integridad de los datos procesados por las computadoras prevalece en forma latente. Por lo que describimos cada uno de los objetivos que contiene esta definición:

a) Salvaguarda de activos

Los activos de una instalación de cómputo incluyen hardware, software, personal, archivos de datos, documentación de los sistemas y papelería, por lo tanto, todos los activos deben ser protegidos por un sistema de control interno, ya que el hardware puede ser dañado intencionalmente, el software y los archivos de datos, pueden ser robados.

b) Integridad de datos

La integridad de datos es un concepto fundamental en la auditoría en informática. Es un estado que implica que los datos tengan ciertos atributos :

- Totalidad
- Veracidad
- Coherencia

Si la integridad de datos no se mantiene, una organización ya no cuenta con una representación de si misma o de los eventos del mundo real. Sin embargo la integridad de datos sólo puede ser lograda a un costo.

Dos factores principales afectan el valor de un elemento de información de una organización:

a) El valor del contenido de información del elemento para la toma de decisiones individuales y

b) El grado en que los datos son compartidos.

El contenido de información de un elemento depende de su habilidad para reducir la incertidumbre que rodea una decisión.

El valor de la reducción de la incertidumbre depende de la remuneración asociada a la decisión a tomar.

c) Efectividad del sistema.

Un sistema de procesamiento de datos efectivo logra sus objetivos.

La evaluación de la efectividad implica tener conocimiento de las necesidades del usuario.

Para poder evaluar si hoy un sistema reporta información de cierta forma que facilite la toma de decisiones a los usuarios, el auditor debe conocer las características del usuario y el entorno de las decisiones por tomar.

La auditoría de efectividad, por lo general ocurre después que el sistema ha estado en operación por un tiempo. La gerencia solicita una auditoría posterior para determinar si un sistema ha alcanzado los objetivos establecidos. Esta evaluación provee información para tomar la decisión si el sistema se desecha, continúa su operación, o bien se modifica de alguna forma.

La auditoría de efectividad también puede ser llevada a cabo durante las etapas de diseño de un sistema. Resulta una tarea muy difícil para los diseñadores de sistemas, asegurarse que los usuarios comuniquen sus necesidades y que entiendan y acepten el diseño propuesto. Si un sistema es complejo y costoso en su implantación, la gerencia puede requerir una evaluación independiente para determinar si es probable que el sistema cumpla con sus objetivos.

El auditor puede ser responsable de efectuar esta evaluación independiente para la gerencia.

d) Eficiencia del sistema.

Un sistema de procesamiento de datos eficiente utiliza recursos mínimos para lograr los resultados requeridos. Los sistemas de procesamiento de datos consumen varios recursos, tiempo de máquina, dispositivos, periféricos, canales, software y trabajo.

Estos recursos son escasos y diferentes sistemas de aplicación compiten para utilizarlos.

La eficiencia en un sistema de aplicación particular, no puede ser considerada aislada de otros sistemas de aplicación. Los problemas de suboptimización ocurren si un sistema es "optimizado" a expensas de otros sistemas.

2.4. AUDITORIA FINANCIERA

Los auditores externos generalmente son responsables de las auditorias financieras, los cuales exploran y verifican el control interno de los diferentes ciclos, como también, los registros en los libros de contabilidad de la empresa, que con base a un previo estudio emiten la conclusión final sobre la confiabilidad de los estados financieros.

El Auditor en Sistemas de Información (ASI) usará frecuentemente procedimientos asistidos por computadora para apoyar a los auditores financieros en la auditoría.

2.5. AUDITORIA OPERACIONAL Y GLOBAL

Una auditoría operacional está diseñada para evaluar la estructura de control interno en un área dada. Los auditores internos están asociados frecuentemente con auditorías operacionales. Muchas auditorías a sistemas de información, incluyendo análisis de controles de aplicación o de sistemas de seguridad lógica, son de naturaleza operacional. Una auditoría global combina los pasos de auditoría financiera y operacional.

2.6. LA AUDITORIA

La auditoría puede ser clasificada de acuerdo a su forma de filiación, de forma individual o por grupo al ejecutar la auditoría.

La auditoría es el proceso de validación de objetivos y la evaluación de resultados a través de pruebas selectivas utilizando elementos de control que verifiquen el grado de correspondencia entre éstos resultados y las metas establecidas en función de los objetivos, aportando conclusiones que permitan retroalimentar al sistema para ajustarlo.

2.6.1. Auditoría Interna

Es una área con funciones específicas con dependencia directa de la alta dirección, la cual examina y valora las actividades de los departamentos como un servicio de la organización.

2.6.2. Auditoría externa

La realizan organizaciones privadas que no forman parte de la organización a auditar y permiten tener, para la organización, un punto de vista crítico, no viciado con la estructura de la organización.

2.7. ADMINISTRACION PARA LA FUNCION DE AUDITORIA EN INFORMATICA

La organizacion de Auditoría en Informática sigue la mayoría de los conceptos utilizados en la organización de muchas otras actividades. La característica peculiar de esta especialidad se basa en dos disciplinas técnicas combinadas que crean la necesidad de reflexionar y seguir conceptos que no son encontrados en otras actividades.

Los conceptos especiales para organizar la actividad de Auditoría de Informática son :

* La planeación efectiva, la operación misma y el control de los recursos que requieren de una combinación de aptitudes gerenciales y técnicas especializadas.

La Informática es una especialidad técnica de servicio que requiere habilidades analíticas y creativas y que ocupa a su personal en actividades especializadas en proyectos de mediano y largo plazo y que generalmente por la demanda y origen del servicio se encuentran alejados del control.

La Auditoría también es un servicio orientado a la asesoría que requiere aptitudes intuitivas y procedimientos más universales y reconocidos donde el sentido común debe ser indispensable, la ocupación de su personal está ubicado en proyectos de menor plazo donde la profundización de conocimientos es menor pero de cobertura mucho mayor.

Ambas características pueden ser complementarias indicando primordialmente que el Auditor en Informática debe cubrir básicamente las cualidades del Auditor aprovechando su experiencia informática y comprender que sus habilidades y satisfacciones como auditor en informática van a ser limitadas, sin embargo, serán substituidas por las que gratifican profesionalmente al Auditor.

* La actividad de Auditoría de Informática en sus funciones de revisión a Centros de Cómputo, Sistemas en Producción, Sistemas en Desarrollo, apoyo a la Auditoría no-Informática, Telecomunicaciones y la propia Auditoría a la Administración de la función de Informática en sí misma, debe estar localizada de tal manera que pueda llegar a dar sus servicios a todo su mercado que se encuentra a lo largo y ancho de cualquier Institución.

* La necesidad de concentrar el conocimiento técnico y experiencia informática genera diversas especialidades por lo que los equipos de Auditoria deberán ser multidisciplinarios.

* La metodología es esencialmente importante tanto para aumentar la productividad y la calidad, como para asegurar la continuidad de la función, por lo que se considera que su creación y mantenimiento es fundamental.

* La estructura organizacional debe dar particular importancia a la planeación, calendarización y control para lograr la economía operacional y los mejores resultados a los auditados.

* La combinación de los requerimientos de desarrollo departamental y operación simultanea debe ser considerada cuidadosamente en la organización y sus funciones, independientemente de los requerimientos de capacitación y administración.

Los conceptos anteriormente mencionados son los que se han tomado en cuenta para establecer en una organización la función de Auditoría en Informática.

2.7.1. Perfil del Auditor de Informática.

Los conocimientos que debe tener un Auditor en Informática se deberán ampliar constantemente de acuerdo con las características de la misma empresa, ya que el grado de tecnología, la centralización o descentralización de las funciones de informática, el medio ambiente y muchos factores más, fijaran las áreas de conocimiento requerido así como su profundidad y especialización.

Los conocimientos y experiencias deseables en un Auditor en Informática son :

* Auditorías Financieras normales (sin aspectos significativos de procesamiento de datos).
* Conocimiento de las políticas y procedimientos de la empresa.
* Conocimientos amplios en técnicas y procedimientos de Auditoría.
* Revisiónes tradicionales de Post - Instalación.
* Revisión de instalaciónes del computador (revisión simple de procedimientos operativos y seguridad).
* Auditoría operacional de Departamentos de Procesamiento de Datos.
* Participación en estudios de factibilidad.
* Revision de controles en el diseño de sistemas.
* Uso de paquetes de Auditoría.
* Consultor de otros Auditores en la utilización de paquetes de Auditoría.
* Desarrollar programas de Auditoría para reportes particulares.
* Consultor en procesamiento de datos o miembro de un grupo responsable del staff de Auditores, incluyendo Auditores en Informática.
* Diseñador de software de Auditoría generalizados.
* Aceptación y pruebas de nuevos sistemas de procesamiento de datos.
* Supervisión de otros Auditores en Informática.
* Conducción de entrenamiento de Auditores en tópicos de procesamiento de datos.
* Uso de DBMS como herramientas de Auditoría.
* Estudios de Análisis de Riesgos.

2.8. FUNCIONES DE LA AUDITORIA EN INFORMATICA

El Departamento de Aditoría de Informática proporciona apoyo en el ejercicio de control a los centros e instalaciones con equipo de procesamiento electrónico de datos y a los sistemas que en esos centros están en producción o en desarrollo. La figura 2.1. muestra las funciones de auditoría en informática.

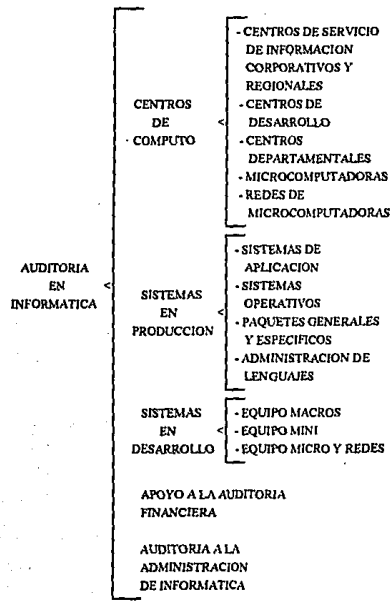


Figura 2.1.

2.9. AREAS A EVALUAR EN UN AMBIENTE COMPUTARIZADO

2.9.1. Areas de Informática

Durante sus inicios, las funciones de auditoría en informática fueron vistas por las áreas de sistemas, como que entorpecían sus labores y no ofrecían ningún producto marginal. Actualmente, las funciones de Auditoría en Informática son contempladas por sistemas, como funciones de apoyo y asesoría que enriquecen la calidad de los sistemas informáticos, obteniéndose una mayor seguridad y apego a las políticas y objetivos de la organización.

2.9.2. Areas Usuarias

En sus inicios, la participación de auditoría en informática fué vista con temor por las áreas usuarias,debido a la creencia errónea de que auditoría detecta errores para despedir empleados.

La buena capacidad técnica y administrativa mostrada por el personal que integra la dirección de auditoría en informática, ha dado como consecuencia que con frecuencia las áreas usuarias soliciten su participación y apoyo en el seguimiento de problemas originados en el medio informático, existiendo una buena comprensión y apoyo a las funciones de la auditoría en informática.

2.9.3. La Alta Dirección

Los buenos resultados obtenidos por la auditoría en informática, la alta dirección se ha percatado de la importancia de éstos resultados para la toma de decisiones, principalmente para aspectos de previsión y control de riesgos relacionados con la posición financiera de la institución, asi como de la salvaguarda y control de sus activos, razones por las cuales con frecuencia se solicita su intervención para la evaluación de asuntos relevantes.

2.9.4. Area de Auditoría No Informática

Con los requerimientos y planes acordados con las direcciones de contraloría, auditoría contable administrativa y auditoría de crédito; la auditoría en informática analiza e implementa soluciones tendientes a solucionar sus necesidades de la información contenida en los archivos de datos de la organización, así como de proporcionar asesoría técnica en la evaluación de problemas originados en el medio informático.

Por las razones citadas, el apoyo proporcionado por la auditoría en informática es relevante en la oportunidad y eficiencia de los resultados manejados por éstas áreas, siendo apreciada su participación, lo que origina una amplia reciprocidad.

ALCANCE DE LAS RELACIONES DE AUDITORIA INFORMATICA DENTRO DE LA ORGANIZACION

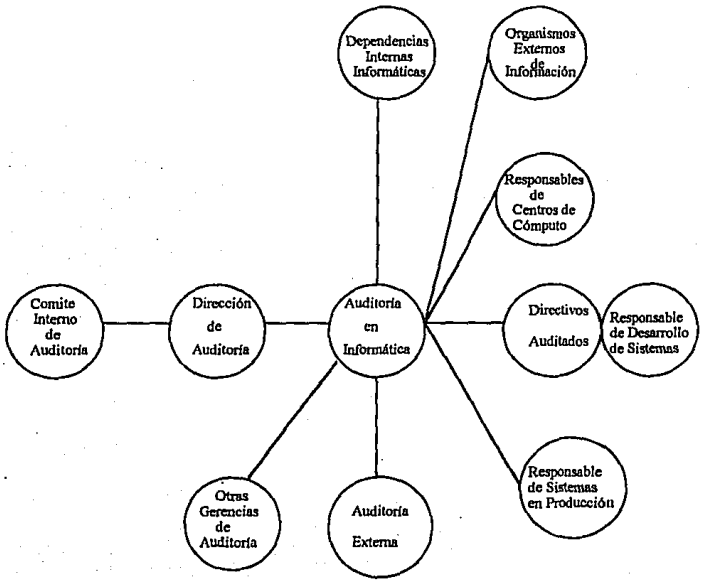


Figura 2.2.

2.10. CODIGO DE ETICA DE LOS AUDITORES EN INFORMATICA

La Fundación de Auditores en Procesamiento de Datos Electrónico (THE EDPAF CODE OF PROFESSIONAL ETHICS, Inc.) da a conocer un código de ética profesional, para guiar la conducta profesional de los miembros de la Asociación de Auditoría de Procesamiento Electónico de Datos (THE EDP AUDITORS ASSOCIATION) y los titulares de la Certificación en Auditoría de Sistemas de Información (CISA).

Los Auditores en Sistemas de Información deben :

* Apoyar el establecimiento y estar de acuerdo con las normas apropiadas, procedimientos y controles para los sistemas de información.

* Cumplir con las normas de la auditoría en sistemas de información.

* Servir al interés de sus directores, accionistas, clientes y público en general de una manera diligente, leal y honesta; y no deberá con conocimiento de causa, pertenecer a ningún grupo con actividades ilegales o impropias.

* Mantener confidencialmente la información obtenida en el curso de sus tareas. La información no deberá ser usada para beneficio personal, tampoco liberada a personas inapropiadas.

* Realizar sus tareas de una manera independiente y objetiva y evitar actividades que amenacen, o puedan aparentemente amenazar su independencia.

* Mantener la competividad en el campo relacionado con auditoría y sistemas de información, a través de la participación en actividades de desarrollo profesional.

2.11. NORMAS GENERALES DE LA EDPAF PARA LA AUDITORIA DE SISTEMAS DE INFORMACION QUE CUBREN INDEPENDENCIA, COMPETENCIA TECNICA, REALIZACION DE TRABAJO Y REPORTE.

Normas generales para la Auditoria de Sistemas de Información :

No. 1: ACTITUD Y APARIENCIA - En todos los asuntos relacionados a la Auditoria, el ASI es independiente al auditado en actitud y apariencia.

No. 2: RELACION ORGANIZACIONAL - La función de la auditoria en sistemas de información es suficientemente independiente del área que esta siendo auditada para permitir la terminación objetiva de la auditoría.

No. 3: CODIGO DE ETICA PROFESIONAL - El ASI cumple el código de ética profesional de la función de auditores de procesamiento electrónico de datos.

No. 4: HABILIDAD Y CONOCIMIENTOS - El auditor es técnicamente competente, posee las habilidades y conocimientos necesarios en la realización del trabajo de auditoría.

No. 5: EDUCACION PROFESIONAL CONTINUA - El auditor mantiene la competencia técnica a través de la educación continua apropiada.

No. 6: PLANEACION Y SUPERVISION - Las auditorias de sistemas de información son planeadas y supervisadas para proporcionar la certeza que los objetivos de auditoria son logrados y la adhesión a estas normas es cumplida.

No. 7: REQUERIMIENTOS DE EVIDENCIA - Durante el curso de la auditoría, el ASI obtiene evidencia de naturaleza y suficiencia para apoyar los hallazgos y conclusiones reportados.

No. 8: DEBIDO CUIDADO PROFESIONAL - El debido cuidado profesional es ejercido en todos los aspectos del trabajo del ASI, incluyendo el cumplimiento de las normas de auditoría aplicables.

No. 9: REPORTE DE COBERTURA DE AUDITORIA - En la preparación de reportes, el auditor establece los objetivos de la auditoría, el periodo cubierto, y la naturaleza y el alcance del trabajo de auditoría realizado.

No. 10: REPORTE DE HALLAZGOS Y CONCLUSIONES - En la preparación de reportes, el auditor en sistemas de información establece los hallazgos y conclusiones concernientes al trabajo de auditoria realizado y cualquier reserva o conclusión que el auditor tiene con respecto a la auditoría.

CAPITULO III

INTRODUCCION

La tecnología ha sido aprovechada para la satisfacción de las necesidades de procesamiento de información y asi poder contar con datos reales, completos y rápidos para la toma de decisiones correcta y efectiva por parte de la alta dirección.

Sin embargo, se presentan muchos problemas en el área de sistemas y básicamente en el centro de cómputo, debido a que no existen procedimientos y controles correctos. Es importante destacar que al momento de hacer una auditoría al áreas de sistemas y al centro de cómputo, éstos resultan con pocas deficiencias o sin ellas. Esto se debe a que los métodos de organización, planeación y administración no son los adecuados o carecen de ellos, esto se presenta por falta de recursos económicos, o por falta de un conocimiento general de lo que representa tener en servicio equipo de cómputo para una organización; pero básicamente se da por la falta de un sistema de control dentro del área de sistemas y centros de cómputo, ya sean pequeños, medianos o grandes.

Una vez teniendo estructurado el sistema de control, la siguiente etapa es corroborar que efectivamente funcione junto a lo planeado. En caso contrario, ver las medidas necesarias y proponer alternativas para su funcionamiento y/o mejora, es en donde la actividad de auditoría realiza un papel muy importante, ya que debe ser un espejo o la misma imagen de lo que está haciendo el sistema de controles, en donde los resultados los contendrá el reporte del auditor (ASI), el cual se dirigirá a la alta dirección.

3. CONTROLES A LOS SISTEMAS DE INFORMACION

Ambos, la computadora y la mente humana son instrumentos maravillosos para grandes realizaciones, pero ambos tienen la capacidad de cometer errores. Porque los errores pueden ocurrir en un centro de cómputo, es esencial entonces que un sistema de controles sea implementado y mantenido.

Definición de un Centro de Cómputo

Podemos definir al centro de cómputo como el conjunto de harware (equipo) y software (programas) a través de los cuales se procesa información. El centro de cómputo es una unidad de servicio y asesoría para las áreas usuarias dentro de una organización.

Surge con el incremento de la demanda de los recursos tecnológicos que ha hecho posible la computadora, recurso que sirve para lograr, superar y satisfacer las metas y objetivos de las organizaciones públicas y privadas, ya que diseña y resuelve formas organizadas de trabajo, con el fin poder utilizar la herramienta, que es la computadora, de una manera racional y con el máximo de aprovechamiento.

3.1. NECESIDADES DE CONTROLAR

En los sistemas manuales y aún en algunos centros de cómputo anteriores los controles fueron ejecutados por una persona que revisaba el trabajo de otra.

Un error no detectado puede tener un serio impacto en el sistema, provocando muchos otros errores. Hay que pensar siempre en errores que pudieran suceder, e intentar divisar los controles que deben ayudar a reducir la probabilidad de su ocurrencia. Día con día, la mayoría de nosotros intentamos incrementar la probabilidad de que cosas buenas sucedan y reducir la probabilidad que las malas cosas sucedan.

De cualquier manera, no se tiene la garantía que lo bueno siempre sucederá. Lo mismo sucede con el desarrollo de un sistema de control, puesto que no existe un sistema infalible.

Los controles son necesarios para un propósito: reducir los riesgos. Antes de poder evaluar los controles dentro de cualquier contexto, debemos identificar los riesgos que los controles deben prevenir, detectar o corregir.

A continuación damos una lista de riesgos a los que puede enfrentarse una empresa:

- Contabilidad errónea
- Pérdida o destrucción de activos
- Costos excesivos/ingresos deficientes
- Sanciones legales
- Fraude y robo
- Decisiones erróneas de la gerencia
- Interrupción del negocio
- Contabilidad inaceptable
- Desventaja ante la competencia

Un riesgo es el efecto de una causa multiplicado por la frecuencia probable de su ocurrencia. Un control actúa para reducir un riesgo, en vez de afectar al riesgo directamente. No existe una relación directa simple entre controles y causas. Por consiguiente varias técnicas de control pueden tener efectos sobre una causa particular, y una causa particular puede ser controlada mediante diversas técnicas. Las áreas generales de las operaciones de un negocio que normalmente son motivo de preocupación son : la información financiera, los activos del negocio y la eficiencia operacional. La introducción del procesamiento electrónico de datos no cambia estas preocupaciones, pero sí modifica las cosas que pueden ocurrir dentro de tales áreas.

3.2. NIVELES DE CONTROL

Un sistema de controles presenta al auditor un dilema por la compleja estructura de su diseño. También demasiados controles y los controles que son muy estrechos, pueden impedir el procesamiento. De otra manera, los controles inadecuados pueden hacer el procesamiento de datos inservible. El incremento directo de controles aumenta la exactitud, integridad y protección del centro de cómputo también como su costo.

La mayoria de los controles pueden también incrementar la efectividad y eficiencia del procesamiento en un punto óptimo después del cual la implementación de más controles resulta inútil.

3.3. CLASIFICACION GENERAL DE LOS CONTROLES

Los controles pueden clasificarse en diversas formas, cada una de ellas nos dice algo distinto respecto a la forma en que los controles y el punto de vista del auditor, cambian en las situaciones del procesamiento de datos.

3.3.1. Controles Verticales y Horizontales

Otra forma de clasificar los controles es dividirlos entre aquellos que siguen las líneas verticales de autoridad de un organigrama y aquellos que siguen los flujos horizontales de procesamiento que cruzan dichas líneas.

La implantación de las computadoras implica en muchas situaciones un giro ascendente de supervisión o del control de la gerencia en línea. Este giro ascendente afecta la naturaleza de los controles verticales debido a que quienes tienen autoridad general sobre los procesos se encuentran en posición más alta dentro de la organización y tienen menos tiempo para ejercer una supervisión detallada.

Por otra parte, en virtud de que ciertos departamentos adicionales participan en un proceso en el que antes participaba un solo departamento, surge la necesidad de más controles horizontales.

Una estructura organizacional que proporcionaba controles adecuados para un sistema manual, normalmente no proporcionará el mismo grado de control para un sistema después de la introducción de una computadora y de aplicaciones integrales.

Esto no quiere decir que los controles verticales, tales como la supervisión y la segregación de funciones, ya no sean importantes para un sistema computarizado; sin embargo, se reduce su efectividad y el énfasis relativo. Tal énfasis debe dirigirse más bien hacia los controles de tipo horizontal, tales como los documentos de envío, las cifras de control y las ediciones.

3.3.2. Controles Preventivos, Detectivos y Correctivos

Esto se refiere a si una determinada técnica de control evitará una causa de riesgo, detectará un hecho ocurrido o corregirá sus defectos después de que ha sido detectada.

Los controles preventivos son aquellos que reducen la frecuencia con que ocurren las causas de riesgo.

Un control preventivo actúa como una guía para ayudar a que las cosas sucedan como deben ser. Con frecuencia son pasivos y no implican ninguna actividad física directa. Por otra parte, tales controles, a menudo permiten cierto porcentaje de violaciones. Los controles preventivos se encuentran a menudo tan sutilmente intercalados dentro de un proceso, que las personas involucradas en la operación pueden no estar concientes de su existencia.

Los controles detectivos no evitan que ocurran las causas de riesgo, sino que, más bien las detectan después de que han ocurrido. No es suficiente la simple detección de una causa de riesgo. Cuando se detectan tales situaciones, deben tomarse una decisión respecto a cual es la acción correctiva apropiada y posteriormente debe llevarse a cabo dicha acción. Un control detectivo no evita que una causa de riesgo ocurra, sin o que dispara una alarma después de que ya ha ocurrido. El control detectivo puede poner fin al procesamiento posterior o simplemente registrar la ocurrencia.

Esta función de vigilancia con frecuencia es bastante confiable; sin embargo, la detección de que una causa ha ocurrido es simplemente eso y nada más. Los controles detectivos alertan a las personas involucradas en el proceso, a fin de que estén concientes de la existencia de una problema. Tal conocimiento es imprescindible si ha de seguirse la acción correspondiente para corregir los defectos de la causa detectada.

El último tipo de control es el correctivo. Este ayuda en la investigación y corrección de las causas de riesgo detectadas. La acción correctiva siempre es necesaria para remediar las causas de riesgo que se detectan. En ciertas ocasiones puede decidirse que no vale la pena seguir una acción correctiva, pero tal decisión debe tomarse consciente y consistentemente, no por negligencia. La alarma que proporciona un control detectivo es inútil si nadie la escucha. Debido a que los controles preventivos son a menudo pasivos (como las instrucciones para llenar una forma), es necesario un control detectivo, para determinar si el control preventivo está funcionando. Aún si así fuese, los controles detectivos seguirán siendo necesarios para detectar los riesgos que evaden el control preventivo. Además las partidas que originan errores son con frecuencia más difíciles de manejar, que las partidas normales; de lo contrario, el error no hubiera ocurrido. La corrección apropiada también puede ser difícil, por lo tanto, todas las partidas que se corrigen, deben procesarse subsecuentemente a través de los mismos controles detectivos, o de otros todavía más estrictos.

No obstante que la corrección sea fácil, sigue existiendo la posibilidad de que se procese en la dirección equivocada, de tal forma que algo que debiera sumarse, en realidad se reste. Los controles detectivos sobre los controles correctivos son esenciales debido a que la corrección del error es en sí misma una actividad altamente propensa a errores.

3.4. PUNTOS DE CONTROL

El centro de cómputo es un recurso valioso para la organización. Existen cuatro puntos que el auditor debe considerar :

- Los controles efectivos deben ser diseñados dentro del sistema, no anexados después.
- En general, los analistas del sistema y programadores no dedican suficiente tiempo para los controles.
- Los auditores deben estar mas envueltos en el desarrollo de sistemas para ayudar a asegurar que los controles apropiados sean implementados.
- Los auditores deben informar a la administración que un sistema de controles no sirve solamente para el concepto de contabilidad adicional de control interno sino que también es importante alcanzar una operación eficiente del centro de cómputo.

Estos controles pueden ser agrupados en cinco categorías generales y definidos como sigue :

Puntos de control relacionados con los sistemas de información

1. Controles Administrativos.

   Estos controles son la responsabilidad de la gerencia del centro de cómputo.

Incluyen funciones tradicionales de administración, tales como establecimiento de planes; reclutamiento, selección, asignación y capacitación de personal; desarrollo, implementación y realización de estándares; y un desarrollo organizacional adecuado.

2. Controles Operacionales.

Estos controles se relacionan directamente con las operaciones de procesamiento de datos y consecuentemente ayudan a asegurar que las transacciones sean manejadas apropiadamente y que los datos sean convertidos exacta y viablemente en información.Estos controles incluyen lo siguiente:

- de entrada
- del sistema operativo
- de procesamiento
- en programas de aplicación
- de manejadores de base de datos
- de hardware
- de operación de la computadora
- de biblioteca y de base de datos
- de salida.

3. Controles de Documentación.

Estos controles se refieren a todas las comunicaciones y documentos que nos dicen cómo operar el sistema. La documentación típica contiene : reportes de desarrollo de sistemas, diagramas de flujo del sistema, lay-outs de archivos, registros y reportes, diagrama de flujo de los programas y tablas de decisión, procedimientos de prueba, listados de programas fuentes y objeto, y procedimientos manuales generales.

4. Controles de Seguridad.

Estos controles incluyen todas las operaciones físicas y de procedimiento utilizadas para asegurar que el centro de cómputo no opere de manera correcta intencional o desintencionalmente por fuerzas internas o externas.

5. Controles Externos.

Estas funciones de control surgen y son realizadas, tanto por grupos de la función de auditoría como de la función consultora, de la alta gerencia, staff especial en grupos de control, y varias personas de la organización.

Los controles ayudan a establecer una supervisión independiente en las actividades generales del centro de cómputo a través del uso del sistema de observación y retroalimentación.

Los controles pueden clasificarse segun su función. Cada una de las clasificaciones nos dice algo distinto respecto a la forma en que los controles y el punto de vista del auditor cambian en las situaciones de procesamiento electrónico de datos.

6. Relación entre Costo/Beneficio de los Controles.

En los sistemas de información, como en cualquier otro sistema, cada control es un factor de costo. Ningún control debe costar más que los errores potenciales. En la medida en que los controles se diseñen inapropiadamente sean excesivos, llegan a ser agobiantes y existe el riesgo de que sean ignorados.

Debe hacerse una revisión para ver si los errores pueden ser descubiertos con anticipación en el ciclo de procesamiento, minimizando :

- Los puntos de control requeridos.
- El daño que puede hacerse a los archivos de datos.
- El trabajo de corrección necesario.

Los controles preventivos son generalmente de más bajo costo. Los controles detectivos normalmente requieren de ciertos gastos operativos. No obstante, los controles correctivos casi siempre son muy costosos, ya que implica más trabajo corregir algo que ocurre en forma inadecuada que hacerlo bien desde el principio.

3.5. CONTROLES ADMINISTRATIVOS PARA EL AREA DE SISTEMAS Y CENTROS DE COMPUTO.

Los controles administrativos se clasifican en tres puntos principalmente :
A continuación se estudiará cada uno para mejorar su entendimiento y comprensión.

3.5.1. Control de la Organización.

El Area de Sistemasy el Centro de Cómputo en la Organización.

Lo primero que tenemos que hacer es definir su ubicación en la organización, hasta haber encontrado su lugar de forma adecuada para proporcionar el mejor servicio y funcionalidad, así como sus características.

Características de un Centro de Cómputo

- Combinar un alto nivel de actividad tecnica con creatividad.
- Requiere una perspectiva detallada en sus etapas de implementación.
- Estar consiente del impacto de su trabajo en las políticas, procedimientos de organización de la institución y aún así mantener un interés en los campos de datos individuales y en la calidad de adaptación de los mismos.

- Mantener la objetividad para encontrar las necesidades de otros o para saber las funciones que se cruzan o abarcan muchas líneas de la organización, aunque organizacionalmente pueda estar situada en un área o ejercer una función específica.

Funcion del Centro de Cómputo.

El centro de cómputo requiere de una organización adecuada, que permita satisfacer las necesidades de los usuarios de una manera eficiente; dicha organización, en virtud de la magnitud que alcanza un centro de cómputo y de la diversidad de servicios que le corresponde prestar, se forma cada vez más compleja y difícil de controlar. El servicio que presta dependerá del nivel, tipo, y manera en que lo desarrolla, por lo que diferirá de una institución a otra.

La ubicación de los centros de cómputo y sistemas depende de forma diferente en una empresa o institución y según sea determinado por la alta dirección o por la dirección general. Las más importantes y comunmente utilizadas se describen a continuación:

Dependencia del Area Financiera.

Esta ubicación es válida, cuando el porcentaje de los trabajos que se desarrollan en el área de sistemas son de tipo administrativo. Pero es importante echar un vistazo de su funcionamiento, ya que, por atender las peticiones de tipo administrativo, descuidaría otras áreas, resultando problemas por no tener ellos las facilidades.

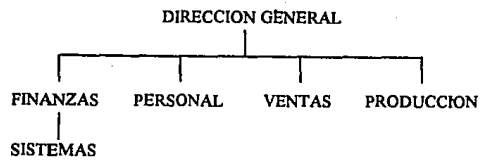


Figura 3.1.

Dependencia del Area de Producción.

Este tipo de ubicación será válida cuando el trabajo desarrollado por el área de sistemas esté encaminado a las necesidades de producción de la empresa.
Esta ubicación no es muy común y sólo en pocas ocasiones llega a justificarse.

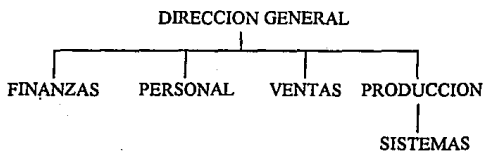


Figura 3.2.

Sistemas como Staff de la Dirección General.

Siendo sistemas una área de apoyo y asesoría a la dirección general por generarse ella información útil para la toma de decisiones, y siendo además una área de servicio a da la organización, la comunicación que debe existir hacia la dirección general es de an importancia para el desarrollo de proyectos acordes a los objetivos de la empresa.

Esta ubicación permite que sistemas tenga la fuerza necesaria para mantener una comunicación a cualquier nivel dentro de la organización lográndose con esto aprovechar positivamente los canales adecuados para proporcionar un servicio eficiente.

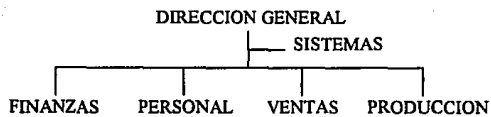


Figura 3.3.

Sistemas como una Dirección dentro de la Empresa.

Para facilitar la comunicación y tenerla en un buen nivel se puede colocar al área de sistemas, como una dirección dentro de la empresa pues así se independizará, y podrá tomar decisiones propias que ayudarán a un mejor trabajo, agregando que cada día toma más adeptos este tipo de organización por ser de las más adecuadas.

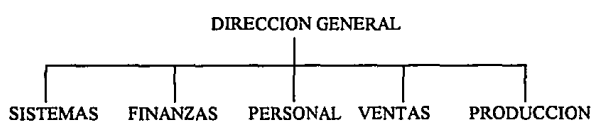


Figura 3.4.

El modelo que se utilice tiene algún impacto en la efectividad de la función; sin embargo, el aspecto clave en el éxito de una área de sistemas e informática es la calidad de su gente y no en la estructura de la organización.

Requerimientos Organizacionales.

En muchas empresas la decisión de iniciar el diseño de un sistema es parte de un plan a largo plazo, el cual puede incluir algunas veces una redefinición parcial de las políticas de la empresa y las metas en los negocios, las cuales pueden resultar en algún grado de reorganización de la empresa. La intención útil de este tipo de reorganización es hacer a la empresa más adaptable al cambio de medio ambiente en el cual opera.

Modelos de centros de cómputo a seguir y su control.

Modelo Centralizado, Ventajas, Desventajas, y Descentralización.

Centralización

Es un modelo en el cual todos los recursos del proceso de información dentro de toda la organización dependen de un solo individuo, sin ir a otros miembros cuyas responsabilidades están más allá del centro de cómputo. Los recursos que reportan a área, no necesariamente deben estar localizadas geográficamente bajo el director, sin embargo hay una relación directa de dependencia a un gerente central de procesamiento de datos. La organización centralizada envuelve la concentración de autoridad y responsabilidad en los niveles más altos de la organización.

Ventajas para la Centralización.

La razón mas frecuente utilizada para la centralización de operaciones es la "Economía de Escala" y ésta, resulta de varios factores:

- Descentralizar computadoras pequeñas puede traernos capacidad sin uso. La Centralización en una computadora de gran tamaño, podría eliminar el costo de tal capacidad sin uso.
- Las pequeñas computadoras individuales pueden ser sobrecargadas generando presión para el uso del equipo o permitiendo tiempo de servicio muy caro.

La centralización en una gran computadora podría absorver esta carga contra la capacidad sin uso de otras microcomputadoras.
- En términos de espacio de piso, electricidad, aire acondicionado y sistemas de seguridad; una gran instalación es menos costosa que múltiples instalaciones pequeñas.
- El número de personal del área, es menor para una gran instalación que para muchas pequeñas.
- Una gran instalación requerirá menos personal ejecutivo que una pequeña.
- Una gran computadora es mas efectiva en costo que una microcomputadora.

La seguridad contra esto es incluir monitores de tv, procedimientos de identificación y de checar entradas/salidas, entrada por una sola puerta, etc.

3.6. CONTROLES DE OPERACION

Los controles operacionales directamente relacionados a las operaciones diarias de procesamiento de datos incluyen :

1. de entrada
2. del sistema operativo
3. del procesamiento
4. en programas de aplicación
5. del sistema de manejo de base de datos
6. integrados a la computadora
7. para la operación de la computadora
8. de biblioteca y base de datos
9. de salida

3.6.1. Controles de Entrada

Se divide en cuatro áreas:

- Códigos de entrada
- Preparación de la entrada
- Verificación de la entrada
- Terminación de la entrada

Código de entrada.

Los sistemas de información actuales no pueden tolerar significados ambiguos o la entrada de datos erróneos en registros computarizados tales como tarjetas de crédito, archivos personales, archivos de inventario, formas de impuestos, ventas, reservaciones en aerolíneas, etc. Antes de autorizar la entrada de datos se debe identificar, clasificar y definir los elementos de datos involucrados.

En cualquier organización, los elementos de los datos (documentos de transacción, campos, registros, archivos, etc.) representan gente, eventos, objetos, etc.

Todos estos elementos individuales son datos para ser grabados y procesados. Por ejemplo, los empleados o bienes en una tienda de departamentos pueden considerarse como datos a capturar, introducirlos al sistema y procesarlos. Es importante que todos los datos procesados por la computadora sean representados apropiadamente e identificados de forma única.

Los códigos proveen una estructura abreviada para clasificar e identificar en forma única datos en la entrada, en la comunicación, proceso, y/o recuperación.

El uso de las computadoras ha dado un fuerte ímpetu a la utilización de códigos, especialmente códigos numéricos y de barra para un control y procesamiento efectivos. Las siguientes son algunas de las más conocidas estructuras de códigos.

a. Códigos secuenciales.

Representa un asignamiento consecutivo de número de artículos tales como chequeras, números de cuenta, artículos de inventario, ordenes de compra, empleados, etc. Es de uso simple, identifica de manera única, és múy útil en muchas aplicaciones de control y puede usarse como código estructurado. Los documentos básicos como cheques, bonos, ordenes de venta, compra y facturas deben tener números secuenciales. Los documentos deben mantenerse fuera del centro de cómputo y cederlos para su procesamiento. Después del procesamiento, las formas deben regresar al área de control responsable. Cualquier forma de dato que no esté bajo control debe rastrearse inmediatamente.

b. Códigos en bloque.

Clasificar artículos dentro de ciertos grupos donde los bloques de número se asignan a clasificaciones particulares. El bloque que representa una clasificación debe situarse sobre la base de una utilización máxima esperada de ese bloque. Por ejemplo, revisar la estructura de códigos de bloque representado a continuación en la figura 3.5.

NUMERO DE CODIGO	CODIGO DE POSICION		
1	Escritorio	Arrendamiento	Contabilidad
2	Silla	Comprar	Mercadotecnia
3	Librero	Rentar	Producción
4	Copiadora	----------	----------

Figura 3.5.

Si un elemento de los datos se introduce en el sistema con un código 421, significa que una copiadora que se ha comprado se asignó al departamento de contabilidad.

Este código también es aplicable al área de contabilidad, donde letras y dígitos pueden representar entre otras cosas la identificación de un artículo, su ubicación en el almacén, el departamento de usuario, etc.

c. Códigos de barra.

Las diferentes configuraciones de barra mostradas en la figura 3.6. son llamados códigos de barra. Los símbolos se pueden leer fácilmente por la computadora y convertirlos en números que representen el código. Cambiando el espesor de las barras y el espacio entre ellas, pueden identificarse de forma única todas la variaciones de productos y tamaños tal y como se muestran a continuación.

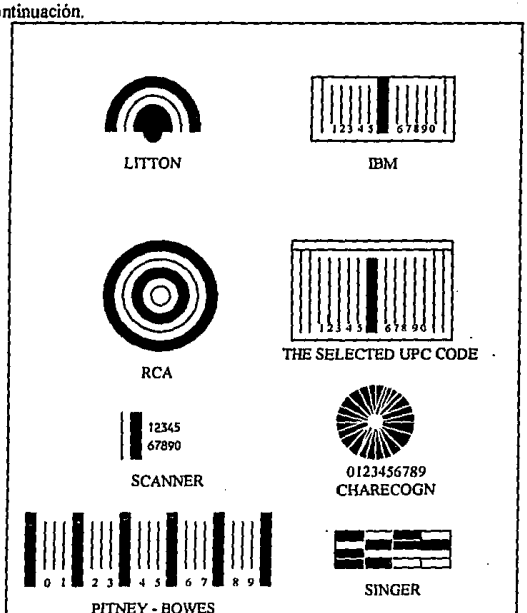


Figura 3.6.

Este código requiere el uso de equipo sofisticado conectado a una computadora. Los artículos contenidos el código de barra se pasan por un rastreador láser, el cual lee el código y le transfiere a la computadora información como precio correcto, tipo, tamaño y otros datos, los cuales son presentados en pantalla e impresos en un boleto de compra al mismo tiempo. El proceso de entrada y contar un artículo toma una fracción de segundo.

Este código permite reducir el tiempo de verificación, actualiza el control de inventarios, elimina el etiquetar los precios y cambiar precios en cada artículo. Reduce la probabilidad de errores humanos, los hurtos y los fraudes en la manipulación de las cajas registradoras.

Preparación de la Entrada.

La preparación de documentos de entrada y transacciones siempre deben ser manejados por personas autorizadas fuera del centro de cómputo. Para asegurar una preparación de entrada apropiada, deben implementarse los siguientes procedimientos :

- Todas las transacciones deben codificarse (por códigos aprobados) por un departamento autorizado.

- Donde sea posible, debe prepararse un control de totales por parte del departamento de origen.

- Formas confidenciales como libretas bancarias, cheques, registros de accionistas deben ser prenumerados y controlados por un funcionario de nivel adecuado.

Verificación de la Entrada.

La introducción de documentos preparada por un empleado debe verificarse o corregirse por otro cuando el resultado de los datos requiera un alto grado de exactitud. La verificación es una operación duplicada y por tanto incrementa el costo de la entrada de datos. Para reducir este costo se puede verificar únicamente los datos críticos tales como totales y números de cuenta, ignorando nombres, direcciones, sexo, etc.

Debe quedar bien claro que la verificación no implica la detección de todos los errores de transcripción. De hecho, los errores se reducen pero no se eliminan totalmente.

Terminación de la Entrada.

Terminar la entrada, significa que toda la entrada que se supone presente y procesada está, lo esté en verdad. Para asegurarse de ello se deben usar controles como los siguientes:

- Control total de la cantidad.

  Se usa para determinar los resultados de algunos cálculos. Se establece normalmente para lotes de un tamaño conveniente tal como un departamento, locación, cuenta o división. Cada lote de registros puede balancearse conforme se procesa. Una acción correctiva si es necesario puede aplicarse a pequeños lotes fácilmente identificables que un gran total. Por ejemplo, en un almacén de departamentos, se graba el total de artículos vendidos y también se hace por departamentos; la suma de éstos últimos debe coincidir con el total del almacén, sino, algún dato está mal.

- Control total del conteo grabado.

Involucra la incorporación de todos los datos de entrada por ejemplo, si hay 100 registros a ser procesados y sólo 99 son leídos, obviamente hay una pérdida; similarmente si hay 100 registros para procesar y el resultado arroja 110, también es erróneo.

Después de que se han contado los registros, el número total de registros se lleva como un control total al inicio y al final del archivo, cambiándose si hay registros añadidos o borrados, balanceando este nuevo total contra el original o el total ajustado. Si el recuento está de acuerdo con el control total, se acepta como prueba de que todos los registros han sido procesados.

3.6.2. Controles de Procesamiento

Consisten en una variedad de técnicas incorporadas en los programas de aplicación para ayudar a asegurar que únicamente los datos válidos o correctos están siendo procesados como se prescribe. Se dividen en dos grupos:

Verificadores de Edición.

Los verificadores de edición ponen en la pantalla de la computadora, errores no detectados causados por omisión, entradas inválidas y otras. Estos verificadores se enlistan a continuación :

- Verificadores numéricos, alfabéticos y de caracteres especiales.

Evitan la entrada de caracteres incorrectos en el procesamiento, por ejemplo la identificación de cierto departamento está formado por los siguientes digitos: 97865. Si por alguna razón se transcribe 97B65 el verificador número detectaría el error antes de efectuar el procesamiento. Otro ejemplo podría ser con los nombres, donde Salmón fue metido como Salmóm.

- Verificador de validez.

La verificación se hace contra tablas u otros datos que aseguren que los datos de entrada son válidos, por ejemplo una tabla de vendedores que la compañía coloca en un archivo en disco magnético bajo estricto control. Cada vez que se paga al vendedor, al dar el número del vendedor, debe encender un número en la tabla de vendedores válidos. Este control de validez, ayuda a reducir la probabilidad de que los pagos se hagan a falsos vendedores.

- Verificadores aritméticos.

Varias rutinas pueden diseñarse dentro de programas de procesamiento para validar el resultado de otros procesos o el valor de campos de datos.

- Dígito verificador.

Cuando un número de cuenta es asignado, un dígito verificador se prepara usando una operación aritmética y anexandolo al número de cuenta. Cada vez que el número de cuenta es introducido para procesamiento, se efectúa el mismo cálculo en la computadora. Si el dígito derivado no es igual al introducirlo al sistema entonces hay un error.

Desarrollo del programa.

Los programas en algunas organizaciones crecen sin ningún control. Frecuentemente los programadores siguen metodologías de desarrollo no muy bien definidas; algunos tratan de codificar antes de que los objetivos estén bien comprendidos y definidos, la participación del ASI es importante para implementar estandares en el desarrollo de sistemas. La metodología para el desarrollo de un programa que debe seguirse se describe a continuación.

- Diseño de lógica.

Antes de hacer cualquier intento para escribir las instrucciones de un programa, la lógica del sistema a programar debe ser comprendida por el programador y aceptados por el usuario. Esta lógica generalmente se prepara con el uso de diagramas de flujo, formatos y tablas de decisión.

- Codificación.

El programador debe convertir la lógica preparada en diagramas de flujo a la sintaxis apropiada de un lenguaje de programación. Selecciona las instrucciones apropiadas y las coloca en secuencia de acuerdo a la lógica descrita en el diagrama de flujo. Cuando la lógica se ha codificado entonces el programa debe probarse para errores sintácticos y lógicos.

- Pruebas.

Los errores del programador son más dificiles de evitar de lo que prodría esperarse. Es raro el programa que trabaje correctamente la primera vez que se maneja con datos de prueba. En la mayoría de los casos deben hacerse varias corridas de prueba antes de encontrar y corregir todos los errores. El compilador encuentra por sí mismo la mayoria de los errores durante la compilación. La prueba real, debe asegurar que el programa no tiene errores lógicos y que es capaz de producir salidas correctas.

- Implementación.

Después de efectuarse los tres primero pasos, se prepara el programa y se instala para ser operado.

- Catalogamiento.

El último paso es catalogar el programa en la librería bajo estricto control. No debe permitir el acceso o cambios al programa sin autorización apropiada.

Documentación del Programa.

Sirve como una referencia que describe todos los aspectos de un programa particular. La documentación mínima debe incluir lo siguiente :

a. Descripción narrada.

Esta descripción debe dar una visión amplia de lo que trata el programa y su propósito.

b. Nombre y número de identificación.

Es simplemente para identificar el programa, da una forma de localizar el programa en la biblioteca.

c. Lógica del programa.

Incluye los diagramas de flujo más las tablas de decisiones si es que hubo.

d. Listados del programa.

Es una copia, generalmente en papel de todas las instrucciones usadas en la codificación del programa.

e. Fecha de prueba y aprobación final.

Fechas de prueba y aprobación, adicionalmente los nombre de las personas que efectuaron las pruebas y el de la persona que las aprobó.

f. Resultados de pruebas.

Los resultados o el listado de la ejecución de pruebas.

g. Formatos de archivos y grabación.

Estas formas describen todas las entradas y salidas.

h. Instrucciones de operación.

Estas instrucciones se despliegan al operador de la computadora, por ejemplo "Montar la cinta No. xxxxxx".

i. Instrucciones para la distribución de la salida.

Estas instrucciones le dicen al personal operativo quién está autorizado para recibir los reportes.

j. Programas autodocumentados.

Esto es quizá lo más importante que debe ser escrito en un programa, de tal manera que permita su fácil comprensión, esto es, deben usarse nombres de las variables que tienen una relación lógica con los datos que están siendo manejados.

Cambios en el programa.

Los cambios no autorizados en un programa representan una de las más significativas amenazas a los sistemas. Es imperativo que cualquier cambio en un programa se haga de acuerdo a procedimientos estrictos de aprobación de cambios y supervisándolos, si éstos son aprobados. Si se realizan cambios autorizados sobre un programa, éste debe probarse para asegurar que hace lo que se supone que tiene que hacer. Una desviación de este procedimiento conduce fácilmente a errores.

Sistema de Manejo de Base de Datos.

Los sistemas de manejo están emergiendo con una pequeña y común base de operación, pero tiene problemas de incompatibilidad. Los programas fuente pueden transferirse de una máquina a otra, o sean transportables, mientras que los archivos sobre los cuales operan los programas no tienen una técnica estándar de almacenamiento.

Subfunciones de los Sistemas de Manejo de la Base de Datos.

Un sistema de manejo de base de datos, comprende una o más de las siguientes subfunciones : manejo de archivos, dudas y generadores de programa.

Abarca las operaciones para la creación de la base de datos, su supresión. Sin embargo, se afirma que la independencia y relación de datos, la no redundancia, integridad, comprensión, seguridad y la auditoría sobre el sistema son también funciones del manejo de archivos.

- Independencia de los datos.

Implica la capacidad de archivar y recuperar datos sin un formato de datos específico. Comunmente, los datos deben ser formateados cuando son archivados.

- Relación de datos.

Implica la construcción de una base de datos con relaciones lógicas entre los inter-registros grabados, además de asociaciones consistentes y lógicas. Por ejemplo, es lógico tener la información concerniente a un individuo dentro de un registro como sigue:

Posición de bytes	01-25	nombre
	26-50	dirección
	51-73	ciudad
	74-75	estado
	76-n	otros datos relevantes

La relación inter-registro significa el uso de técnicas de dirección tales como encadenar o invertir archivos de tal forma que registros con información similar pueden obtenerse sin necesidad de revisar el archivo entero. Las relaciones que pueden existir entre los datos que están en la base de datos deben quedar claramente especificadas para que se puedan derivar las asociaciones deseadas.

- No redundancia de datos.

Implica el almacenamiento de los mismos datos en más de una locación de un dispositivo de almacenamiento. Es costosa, no únicamente desde el punto de vista de una utilidad deficiente de espacio almacenado, sino desde el punto de vista del procesamiento, ya que más información irrelevante debe manejarse durante el procesamiento. Por tanto, desde el punto de vista del costo de almacenaje y tiempo de máquina, la base de datos debe evitar la redundancia de datos.

- Integridad de los datos.

Implica datos libres de error. Una base de datos implica a muchos usuarios y es de extrema importancia que el sistema sea capaz de prevenir la contaminación de los datos, en el tiempo de captura. Es importante recordar que los errores se hacen tanto en la captura de nuevos datos, como en datos que serán dados de alta. Numerosas técnicas para reducir errores están disponibles estos, incluyen el uso de dígitos verificadores, validación del tamaño, etc.

- Seguridad de los datos.

La dificultad de tener acceso a los datos debe ser función de la confidencialidad de los datos y la autoridad del usuario. Se debe dar seguridad hasta en el nivel más elemental.

La prevención del acceso no autorizado a los datos es sólo una de las múltiples facetas de la seguridad. La probabilidad de pérdida de datos debido a robos, fuego, etc.; es grande.

- Auditoría sobre el sistema.

Poder hacer una auditoria sobre el sistema se convierte en un aspecto extremadamente importante en los sistemas que manejan base de datos, ya que los auditores deben verificar que todas las transacciones se están recibiendo apropiadamente, además de que la entrada y todos los datos que residen en la base de datos se han modificado apropiadamente.

Estos sistemas generalmente tienen capacidades auditoras internas, las cuales pueden servir a los auditores, Por ejemplo, IMS (el controlador de la base de datos de IBM) tiene procedimientos que registran todas las entradas y salidas, así como imágenes de antes y después de los registros modificados en la base de datos.

3.6.3. Controles de Biblioteca y Base de Datos.

La biblioteca y la base de datos representan la base del sistema de información y deben ser controlados.

Si hay pérdida o destrucción deben haber sido establecidos procedimientos preplaneados para reproducir cualquier dato perdido. Se dividen en dos grupos :

- Físicos
- De procedimiento.

Controles Físicos.

El fuego, inundaciones, robos, empleados resentidos, motines y plagas entre otros, representan peligro para la información vital de una organización. Un almacén seguro ara ésta información es de gran importancia para la operación continua de cualquier equipo de cómputo. Los dispositivos para la protección como anillos protectores para cintas magnéticas, deben usarse para prevenir borraduras accidentales. Todos los dispositivos de almacenamiento, deben mantenerse libres de contaminantes ambientales, así como controlarse estrictamente las condiciones de humedad y temperatura.

Controles de Procedimiento.

Todos los archivos deben guardarse en una biblioteca aún cuando no se usen.

La biblioteca debe tener un registro completo de todos los archivos en una lista de inventario, a qué persona están asignados los archivos, el estatus y cuando han sido regresados. Todos los archivos deben contener etiquetas externas para su identificación, las cuales deben estar en claves indescifrables. La limpieza y reparación deben hacerse regularmente a cintas y discos magnéticos. Tal procedimiento minimiza los errores de lectura/escritura y asegura un suministro adecuado de medios de almacenamiento de archivos recomendable para archivos secuenciales.

Con dispositivos de almacenamiento de acceso directo como discos y cintas magnéticas, es recomendable que los contenidos sean escritos periódicamente y en un archivo de respaldo y almacenados en otro sitio. Adicionalmente debe llevarse una bitácora de transacciones por dos razones; una, porque constantemente hay transacciones y la bitácora puede enlazar un respaldo con el siguiente; y dos, al escribir sobre un disco o cinta magnética, se cubre lo que había.

3.6.4. Controles de Salida.

Los controles de salida se establecen como un chequeo final sobre la información procesada. Estos procesos son :

- Las salidas deben encauzarse inmediatamente a una área controlada y distribuirse únicamente a personas autorizadas por personas autorizadas.
- Los controles totales de salida deben ser compatibles con los controles totales de entrada para asegurar que no hay datos que se hayan perdido o añadido durante el procesamiento o la transmisión.
- Todas las formas de control deben ser prenumeradas y contadas, como ejemplo los cheques de pago.
- Cualquier salida de alta confidencialidad que no deba ser accesible al personal del Centro de Cómputo, debe generarse a través de un dispositivo de salida por ejemplo, una impresora en un locación segura fuera del cuarto de cómputo.
- A pesar de todas las precauciones tomadas se dan errores.

El mejor punto de control para detectar errores es el usuario. Por tanto, los procedimientos deben establecerse por un auditor que coloque un canal entre el usuario y el grupo de control para el reporte sistemático de errores o impropiedades.

El diseño de tales sistemas utilizaria un enlace de retroalimentación en el cual los usuarios reportan todos los errores al grupo de control y éste a su vez tomaría la acción para corregir cualquier inexactitud e inconsistencia que pueda presentarse. Hay otros controles de salida, tales como los chequeos manuales sistemáticos, muestreo estadístico, conteos físicos de inventario. Puede observarse muchos métodos de control de salida, pero el nivel de control debe estar en función de la confidencialidad de la salida.

La degradación de uno de los controles puede ocasionar que se comprometa el sistema entero. Por tanto el auditor debe estar alerta y evaluar cuidadosamente cada uno de los controles operativos.

3.7. CONTROLES DE DOCUMENTACION

La documentación adecuada de los sistemas de computadora, los programas, la operación y otros procedimientos relativos, son necesarios para la comprensión completa y exacta de las actividades de procesamiento en computadora y del impacto de tal procesamiento en los grupos usuarios.

La documentación se utiliza para proporcionar a la gerencia las bases para entender claramente los objetivos del sistema, los conceptos y los resultados y para asegurar que las políticas se cumplan, con objeto de servir como base para la revisión de la contabilidad y de los controles internos, por parte de los auditores internos y externos y proporcionar una referencia conveniente a los analistas de sistemas y a los programadores responsables del mantenimiento de los sistemas y de los programas existentes.

Mientras que la necesidad de la documentación es generalmente aceptada, su cumplimiento en la práctica varía considerablemente, existiendo desde organizaciones en

donde todo queda archivado en la memoria de los programadores, hasta aquellos que no permiten el inicio de un nuevo proceso, antes de que la documentación completa haya sido elaborada y verificada.

La preparación de un mínimo de documentación requiere una cantidad apreciable de tiempo y esfuerzo por parte de los analistas de sistemas y programadores, lo que, al enfrentarse a presiones en la realización de su trabajo, frecuentemente resulta el primer obstáculo.

En la práctica, las modificaciones a los programas en los casos en que la persona que lo describió no está disponible y no existe la documentación adecuada, con frecuencia significa una lenta y costosa reconstrucción de la lógica del programa seguida por una revisión del programa o inclusive la vuelta a planear y codificar el mismo.

Si en una organización, la documentación de sus procesos en computadora debe de cumplir con estos objetivos, no solamente deberá estar completa, sino que también deberá ser consistente para todos los sistemas, independientemente de quién la preparó, por ejemplo, esta debe ser preparada de acuerdo con estándares pre-determinados. A causa del alto índice de problemas que pueden presentarse y la variedad de equipo y lenguajes de programación existentes, no se cuenta con estándares de documentación completos y universales.

Por consiguiente, toda la organización que esté planeando la introducción del procesamiento en computadora, deberá establecer estándares adecuados de documentación previos a la iniciación del diseño y la programación de los sistemas.

3.7.1. Asegurar que la Documentación Adecuada Exista y Sea Controlada Correctamente.

Estándares Mínimos de Control.

Deberá existir un comite que revise y evalue que se preparó toda la documentación de acuerdo con los estándares predeterminados.

Los estándares en el centro de cómputo, son las normas bajo las cuales deben de trabajar los analistas de sistemas, programadores, operadores de computadora y demás personas involucradas en el procesamiento por computadora.

Cada organización deberá establecer sus propios estandares de procesamiento de datos que reflejen sus requerimientos y circunstancias propias. Todos los estándares decididos por una organización, deberán publicarse para formar parte de un Manual de Estándares y Procedimientos, el cual se deberán de distribuir copias a todo el personal interesado, por ejemplo, analistas de sistemas, programadores, operadores de la computadora, departamentos usuarios, administradores y auditores.

Los estándares deberán ser revisados, actualizados regularmente y modificados cuando resulte necesario, con el fin de asegurar que reflejen con exactitud las politicas en uso.

La técnicas de control se enfocan a:

* de documentación de sistemas.
* de documentación de la programación.

de documentación de los programas.

Estándares para la elaboración de la documentación de las operaciones.

Estos estándares para la documentación individual de programas se aplican en forma adicional a los estándares generales de operación para actividades como el manejo de las cintas magnéticas, operación de la máquina, mantenimiento del equipo y otras actividades normales de operación.

* Se deben establecer estándares de documentación para la preparación de instructivos para las personas que se responsabilicen del control sobre los datos de entrada y salida de la computadora (grupo de control y grupos de usuarios).

3.7.2. Asegurar que Todos los Sistemas Sean Documentados Correctamente.

Estándares Mínimos de Control

Debe existir un comite que asegure la solución de un problema éste sea resuelto y establecido en forma clara y exacta.

El diseño de sistemas de procesamiento en computadora, sólo podrá ser controlado efectivamente cuando haya una definición clara y confiable de los requerimientos y objetivos de procesamiento del área en revisión.

Normalmente los sistemas comerciales de procesamiento de datos, son diseñados por analistas de sistemas, que carecen de experiencia en los departamentos usuarios y que en el mejor de los casos no se sentirán responsables por llevar adelante el sistema.

Un control efectivo acerca de nuevas soluciones a los problemas de procesamiento, se obtendrá sólo haciendo que el analista de sistemas produzca la documentación de los componentes del sistema, en forma que el mismo pueda ser revisado por la gerencia, los usuarios potenciales, así como los auditores.

Técnicas de Control.

* Se deberá hacer una difusión del problema para cada problema de procesamiento o área de aplicación general.

  La elaboración de una definición del problema, proporcionará un medio por el cual la administración y otros grupos interesados, puedan revisar la definición del problema y así saber de antemano que cambios de política podrá llevar en paralelo a la instrucción del procesamiento en computadora, y también servirá para evitar que se realicen diseños de sistemas sin autorización.

* Se deberá preparar la documentación de sistemas para cada aplicación.

La documentación de sistemas, normalmente es preparada para un sistema completo o un sub-sistema bien definido, más que para un programa de cómputo individual.

* La documentación de los sistemas deberá incluir descripciones de las funciones de control, de los procedimientos y de las responsabilidades, en forma clara y completa.

Los controles de procesamiento sólo podrán funcionar en forma adecuada, cuando los procedimientos de control hayan sido documentados convenientemente y comprendidos por las personas responsables de su implantación.

3.7.3. Asegurar que Todos los Programas Sean Documentados Correctamente.

Estándar Mínimo de Control

Se deberán de diseñar procedimientos para asegurar que los documentos y registros de los programas sean completos para una clara compresión del mismo.

Los programas, una vez terminados pudieran no producir los resultados que se desean debido a que el programador no entendió debidamente el problema o errores u omisiones. Un control efectivo sobre las correcciones y revisiones a los programas, así como proveer un medio aceptable para revisiones por otros grupos interesados, solamente se podrá obtener si existe una documentación aceptable.

Técnicas de Control

Para cada programa se deberá elaborar la documentación adecuada de la programación.

Una instalación de computadora debe proporcionar las facilidades para revisarla y cuando resulte necesario, revisar los programas. La descripción del programa, de los registros y las instrucciones para operación, debe completarlas el programador, quien es responsable en un programa, en forma tal que otro programador pueda entender el mismo y realizar las modificaciones a éste. Esto solamente se podrá realizar con la propiedad indispensable si cada programa cuenta con la documentación adecuada.

3.7.4. Procedimientos e Instrucciones para Todo el Personal de Procesamientos de Datos y Personal del Departamento Usuario, que Sean Documentados Correctamente.

Estándares Mínimos de Control

Deben tener procedimientos que aseguren la disponibilidad de toda la información requerida por el operador de la computadora para el cumplimiento de sus funciones y responsabilidades.

Normalmente los operadores de una computadora, trabajan con muchos programas elaborados por distintos programadores. El resultado correcto de la ejecución de estos programas no deberá depender de que el operador tenga en su memoria los requerimientos acerca de la operación de cada uno de ellos. Unicamente se alcanzará un control efectivo sobre las operaciones de la computadora cuando existan instrucciones de operación adecuada, preparadas de acuerdo con estándares predeterminados.

Deberán existir procedimientos que aseguren la disponibilidad de la información necesaria para entender completamente las operaciones de mantenimiento y protección de errores.

Los archivos pueden destruirse, mantenerse más allá del plazo debido o extraviarse, salvo que se proporcione a las personas que se responsabilicen de los mismos, instrucciones claras y completas referentes a procedimientos tales como : control de archivos, fechas de vigencias, disponibilidad, reconstrucción y requisitos de seguridad de los mismos.

Se contará con procedimientos que aseguren la disponibilidad de la información necesaria para las personas que se responsabilicen de controlar las entradas y las salidas de la computadora.

Deberán documentarse las responsabilidades del grupo de control, acerca de cada sistema. Las instrucciones deberán de ser claras y completas y seguirse en todos los casos.

Deberá haber algún método que asegure que esté disponible toda la información requerida por los departamentos que proporcionan datos o que reciben información de la computadora.

El éxito de procesamiento en la computadora, dependerá de la puntualidad con que se efectúe la recepción de los datos de entrada, de que los mismos sean confiables y de que estén completos. Sólo se obtendrá un control efectivo acerca de los datos de entrada, mediante la adopción de instrucciones claras y completas a los departamentos interesados y su cumplimiento.

Técnicas de Control

Para cada programa deberán elaborarse instrucciones de operación.

Deberá ser posible para cualquier operador llevar a cabo las operaciones de procesamiento de cualquier programa a pesar de no tener experiencia previa acerca del programa en particular. Esto será posible únicamente asegurándose de que las instrucciones de operación adecuada las elaboren los programadores por todos los programas que reciban.

Además de las instrucciones de operación individuales para cada programa, los operadores de la computadora deberán contar con instrucciones detalladas acerca de sus responsabilidades en general y las acciones que deben emprender bajo circunstancias específicas.

Se deberán preparar instrucciones acerca del control de los archivos de cada sistema y ponerlas a la disposición de la persona encargada de la salvaguarda de los archivos.

La documentación de los sistemas deberá comprender una sección acerca de los procedimientos de control de archivos, una copia de la cual deberá estar disponible en la biblioteca.

Las personas que asumen la responsabilidad de la custodia y seguridad de los archivos, deberán contar con instrucciones por escrito claras y completas.

Se deberán elaborar instrucciones sobre control de los datos por cada sistema y hacerlas del conocimiento de las personas encargadas del control de los datos.

Las personas encargadas del control de los datos de entrada y salida pudieran estar en un grupo de control separado, en el grupo de operaciones de la computadora, o tratarse de empleados de los departamentos usuarios. Independientemente de quien realice la función, las instrucciones necesarias deberán formar parte de la documentación del sistema y hacerse del conocimiento de la persona apropiada.

Se deberán elaborar instrucciones por cada sistema al departamento usuario y hacerlas del conocimiento de los departamentos interesados.

3.8. CONTROLES DE SEGURIDAD.

Generalmente, los controles de seguridad no afectan el procesamiento apropiado y preciso de transacciones tanto como los controles anteriores.

Conceptualmente, un sistema seguro es uno que está a prueba de todo. Los controles de seguridad ayudan a protegerlo contra fallas de hardware, software y gente. La ausencia de estos controles, puede incrementar la probabilidad de errores, tales como :

- Operaciones degradadas
- Sistema comprometido
- Pérdida de servicios
- Pérdida de activos
- Pérdida de declaraciones no autorizadas de información especial.

Los controles de seguridad, así también como todos los controles expuestos antes, se aplican a pequeños centros de cómputo, grandes y sofisticados sistemas de cómputo y otros servicios de computadoras.

Estos controles son un punto clave, ya que ellos no pueden ser rechazados por el auditor.

El control de seguridad está dividido en tres categorías:

- Peligros
- Técnicas de seguridad física
- Técnicas de procedimiento de seguridad

3.8.1. Peligros.

Un peligro representa un riesgo de pérdida o daño. Lo opuesto al peligro es la seguridad. En los sistemas de información como en otros sistemas, hay usualmente una jerarquía de peligros, proporcionaremos las jerarquías de peligros y las metas de control contra éstos.

Tipos de Peligros.

Los tipos de peligro en un centro de cómputo están dadas por su ocurrencia y su impacto. Además, en cualquier sistema en particular, la manera en que se representan estos peligros es muy diferente.

- Mal funcionamiento.

  Los errores de la gente, el software y del hardware, provocan los problemas más grandes, actos de omisión, negligencia e incompetencia, causan más daño que todas las áreas juntas.

- Fraudes y accesos no autorizados.

  Este peligro es el logro de acciones a través de lo deshonesto, del engaño o embuste. El fraude puede ocurrir por :

- Infiltración y espionaje industrial
- Bloqueando las líneas de comunicación de datos
- Recepción de datos de receptores parabólicos
- Curiosear archivos de usuarios en terminales
- Entrar al sistema con clave de otro usuario
- Confiscación física de archivos y otros documentos

- Energía y fallas de comunicación.

En algunos lados, este peligro puede ocurrir con gran frecuencia, más que otros peligros. Para un gran alcance, la factibilidad y confiabilidad de la energía y las facilidades de comunicación, son una función de la localidad. Los apagones ocurren frecuentemente en época de lluvias y esto se debe contemplar. Si el suministro de la energía no es el conveniente, puede quemar los componentes y dañar la computadora. Este peligro puede ser fácilmente controlado con un regulador de voltaje y con un sistema de energía ininterrumpible. También, durante las horas de trabajo, los canales de comunicación están a veces ocupados y/o con ruido.

- Fuegos

Los incendios ocurren con más frecuencia de lo que se piensa y pueden ser desastrosos. Se deben considerar los fuegos causados accidentalmente así como los premeditados.

- Sabotaje y motín.

Se ha tenido casos donde los centros de cómputo instalados en áreas urbanas han sido dañados. Pero la ubicación no es siempre un factor clave; también lo pueden ser bombas y de ahí resultar pérdidas económicas y hasta vidas humanas.

- Desastres naturales.

Los terremotos, huracanes, inundaciones, trombas, rayos, etc., son devastadores. El sentido común y la planeación ayudarán a reducir el daño que puedan causar. Como se vió el 19 de septiembre de 1985, fecha que todo México recuerda con tristeza y que debido al terremoto, también para el aspecto computacional fue fatal para el sector público, puesto que sus centros de cómputo, estaban instalados en las áreas más afectadas y que a la fecha no se han podido recuperar totalmente.

- Peligros generales.

Esta categoría cubre peligros aleatorios que son difíciles de definir y anticipar. Normalmente, el sentido común y las seguridades generales disminuirán su ocurrencia. Por ejemplo, un accidente cerca del local del centro de cómputo se remediaría con una buena planeación del sitio donde se implantará el centro de cómputo.

Metas de los controles de seguridad contra los peligros.

Las metas de los controles de seguridad contra los peligros pueden ser vistos como una serie de niveles de controles. Esto es, si un nivel falla, entonces otro nivel lo toma y así sucesivamente, y el impacto en el sistema se reduce.

1o. Disuadir. En este nivel, la meta es la de prevenir cualquier pérdida o desastre que pueda ocurrir.

2o. Detectar. La meta es la de establecer métodos de monitoreo y observación para los peligros y reportarlos para la acción correctiva.

3o. Minimizar	El impacto de desastre o pérdida. Si un accidente o desgracia ocurre, deberá haber procedimientos establecidos y facilidades que ayuden a reducir las pérdidas. Por ejemplo, un respaldo del archivo maestro nos ayudará a reducir la destrucción del archivo maestro principal.
4o. Investigación.	Si una pérdida ocurre, se debe hacer una investigación inmediatamente para determinar que sucedió. La información obtenida de la investigación puede ser usada para la planeación de la seguridad a futuro.
5o. Recuperación.	Debe haber un plan de acción para recuperar desde la pérdida y comenzar operaciones tan pronto como sea posible.

3.8.2. Técnicas de Seguridad Física.

Incluyen dispositivos y localización física de las facilidades de cómputo que ayuden a resguardarse contra los peligros. Estas Técnicas son :

- Acceso físico controlado
- Posición física
- Dispositivos de protección física

Acceso Físico Controlado.

La protección de control de acceso es básica para un sistema de seguridad. Si personal no autorizado no puede entrar a las facilidades de la computadora, entonces la oportunidad de perjuicio es reducida considerablemente, los siguientes puntos ayudan a controlar el acceso.

- Guardias y escolta especial .

Los guardias deben ser localizados en puntos de entrada estratégicos del centro de cómputo, todos los visitantes que tengan permiso para entrar deben ser acompañados por una persona designada.

- Registros de entrada/salida.

Todas las personas deben firmar un registro indicando la fecha, nombre, hora de entrada y salida, propósito de la visita y firma.

- Gafetes.

Codificados por color, con una fotografía en lugar visible y es utilizado para identificar personal autorizado y a visitantes.

- Tarjetas de Entrada/Salida

El control de tarjetas en su equipo, es usado solo en conjunción con otras medidas, es probablemente el dispositivo de acceso más eficiente. Las puertas del centro de cómputo se abrirán con tarjetas codificadas óptica o magnéticamente, la autorización de entrada puede ser controlada dinámicamente por puertas individuales, tiempo del día, día de la semana y clasificación de seguridad de los individuos a quienes de les fue dada la tarjeta. Las autorizaciones pueden ser fácilmente aumentadas, borradas, y las actividades de entrada son puesta en un reporte para un control oficial.

Los estados de abierto y cerrado de las puertas pueden ser monitoreadas, e intentar una entrada no autorizada, puede ser detectada inmediatamente y una alarma sonará.

- Monitores de Circuito Cerrado.

Los dispositivos de monitores de circuito cerrado de t.v. y cámaras son conectadas a un panel de control, para ser vigiladas por personal de seguridad, éstas son muy populares. Son muy efectivos para controlar una área múy grande concentrándolos en puntos de entrada y salida.

- Papel Destrozado.

Los reportes nunca deben arrojarse al bote de la basura. En un sin fin de casos, los ladrones pudieron robar información confidencial obteniéndolos del depósito de basura. Cualquier reporte si se va a tirar, se debe triturar en caso de no tener máquina trituradora, se debe despedazarlo hasta hacerlo confeti y así no podrá ser reconstruido.

- Entrada con Doble Puerta.

La primera puerta permite el acceso a los servicios de cómputo, la segunda puerta tiene que ser abierta para entrar al cuarto donde se encuentra la máquina.

- Puertas de Emergencia abatibles en un sólo sentido.

Los dispositivos antes mencionados pueden ser combinados con otros

medios de seguridad. Por ejemplo, la tarjeta puede ser combinada con un identificador de geometría de manos.

Posición Física.

La posición del centro de cómputo es una consideración importante en la planeación de la seguridad. Debe tener los siguientes lineamientos :

- Posición Remota.

El sitio de la computadora debe ser localizado lejos de aeropuertos, equipos eléctricos (radares, micro-ondas), áreas urbanas decadentes, tráficos pesados, calentadores de vapor, etc., si el sitio no puede estar tan remoto como sea deseable, se puede localizar en un punto donde se tenga un radio de 60 a 100 metros y que no tenga nada que ver con el exterior instalando alrededor de él, reflectores y una cerca en su perímetro.

- Edificio Separado.

Muchos especialistas en seguridad recomiendan que el centro de cómputo sea encasillado en un edificio separados; cuando ocupa un edificio separado, el control de acceso es más fácil, y hay menos riesgo de peligros generales. Por ejemplo, hay menos riesgo de daños de agua o provocados por fuego de productos inflamables utilizados por otros ocupantes. La desventaja de un edificio separado es que un ataque deliberado en la fuente de poder, líneas de comunicación y suministros de agua pueden ser más fáciles porque el centro de cómputo está encasillado en una estructura específica.

Si el centro de cómputo, no está encasillado, entonces debe estar en el centro del edificio, lejos de paredes y no se ubicará en las plantas altas y bajas, no debe ser hecho como un aparador o una vitrina.

- Identificación.

El sitio de la computadora no debe contener ningún signo que lo identifique al exterior.

- Control del Equipo Accesorio.

La energía y las líneas de comunicación deben ser localizadas bajo tierra. Los dispositivos de tomas de aire, compresoras y torres de enfriamiento deben ser protegidas con barreras y/o localizadas en alturas que no puedan ser alcanzadas fácilmente.

- Posición de las Facilidades de Respaldo.

El respaldo juega un papel muy importante en muchas áreas del sistema total de control y es el elemento clave de recuperación. Las facilidades de respaldo deben estar lo suficientemente lejos del centro principal para salvarse de los mismos peligros, poderse recuperar rápidamente y ser útil, el sitio donde se localizan los respaldos debe ser confidencial.

Dispositivos de Protección Física

Los dispositivos adicionales de protección deben ser considerados en un plan de protección general con los puntos siguientes :

- Drenajes y Bombas de Agua.

Algunas veces los tubos de agua se revientan o el agua en la extinción de un fuego o inundación amenazan a un centro de cómputo. Para ayudar a reducir el impacto de estos percances, los drenajes y bombas de agua deben ser instalados lejos del centro de cómputo.

- Energía de Emergencia.

De nueva cuenta, el respaldo juega una parte importante en el control. Los UPS (Uninterrumpible Power System) que significa sistema de energía ininterrumpible, este debe ser instalado para respaldo de energía para proveer procesamiento continuo. Esto depende hasta de la frecuencia y naturaleza de las variaciones de energía y el efecto que tienen en el centro de cómputo. Las fallas de energía o variaciones pueden ir de pocos milisegundos o en lapsos de gran tiempo. Estas fluctuaciones de energía pueden resultar en pérdidas de datos, errores en el procesamiento, tiempo perdido, mal funcionamiento del equipo, daños, etc.

Un estudio completo de fallas de energía deben ser hechas para determinar las causas de cualquier variación, para centros de cómputo menores se puede eliminar con un equipo generador de energía o con reguladores de voltaje.

Pero hay que recordar que cualquier interrupción puede ser crítica y producir muchos efectos no deseados.

Aunque un UPS no puede ser justificada en algunos lugares estables, en un futuro pueden fallar.

- Cubiertas.

Todos los equipos deben ser protegidos con cubiertas de plástico cuando no se utilicen, en muchos casos los daños por agua en equipo de cómputo se reducen durante un fuego porque el equipo fue tapado y no penetró en él el agua.

- Control de fuego.

Existen 3 clases de fuego :

Clase A - Celulosa
Clase B - Líquidos flamables
Clase C - Eléctrico

Por lo general, el centro de cómputo maneja las clases A y C, por lo que, necesitan detectores de humo y métodos de extinción.

Se recomiendan los siguientes extinguidores con base a costo y tamaño del Centro de Cómputo.

* Extinguidores portátiles de Bióxido de Carbono o HALON.
* Gas flourido
* Sistemas con HALON (no provoca daños a humanos y es el mejor de todos los medios de extinsión, preferencialmente el 1301).
* Sistemas con CD2 (con bióxido de carbono, es el indicado para la clase C, pero puede sofocar al personal).
* Rociadores de agua.
* Sistemas de extinción de humo (a veces es un gran problema, más que el fuego, porque el material que se quema es tóxico como el plástico y el vinil).

Para los sistemas de extinción, el personal debe percatarse de que realmente es importante el fuego y encender el sistema en el panel de control y habiéndose encendido las alarmas audibles y visibles para comunicarse además con la Central de Bomberos.

- Seguridad del edificio en general.

Las paredes del edificio deben ser construídas con concreto. Paredes y techos deben tener al menos un rango de una hora de soporte al fuego directo. El número de puertas debe ser limitado, no tendrá ventanas y debe contener ductos de humo.

3.8.3. Técnicas de Procedimientos de Seguridad.

Es difícil la diversión entre técnicas de seguridad física y por procedimientos, porque hay mucho de común entre los dos.

Una técnica puede trabajar en conjunción con otra, y engrandecer la efectividad de las demás. En mayor instancia, una técnica de seguridad por procedimiento es nada más que el uso de una técnica de seguridad física.

En donde las técnicas de seguridad físicas con fuegos, desastres naturales, etc., y las técnicas de seguridad por procedimiento son casi exclusivamente para el control de acceso, se requerirán de las siguientes técnicas de seguridad físicas :

- Integridad
- Aislamiento
- Identificación
- Autorización
- Autenticidad
- Monitoreo
- Integridad

Significa que el sistema es confiable y dependiente. Como un concepto en los controles de seguridad, la integridad es básicamente el aseguramiento de que el sistema está funcionando en forma completa y correcta. La ausencia de integridad ocasionará que los demás conceptos no sean efectivos.

Aislamiento

En los centros de cómputo, el aislamiento debe ser mantenido entre los usuarios y la información. También entre los recursos, el hardware, el software y los procesos.

Este concepto reconoce y trata con el incremento de compartimiento simultáneo de facilidades y procesos y el uso extensivo de redes de comunicación de datos en los sistemas de cómputo de hoy en día.

El procesamiento concurrente de diferentes usuarios, requiere la separación y protección de información individual y de los procesos de trabajo. El incremento en el uso de redes de comunicación de datos ha abierto otras exposiciones que deben ser protegidas. Muchos procedimientos de protección que afectan el aislamiento son los siguientes :

- Desconexión y separación. Una forma de que el aislamiento de alcance por distribución geográfica y lógica en la cual no hay conexiones entre ciertos elementos del sistema.

  Aunque existen relaciones que deben permanecer como las de operador/consola, operador/programa, programa/computadora, analista/programa, usuario/terminal, etc. Por lo tanto, para tener aislamiento debemos evitar cierto tipo de combinaciones.
- Acceso de privilegio mínimo. El privilegio asignado debe ser apropiado para el usuario y tener la autoridad mínima de acceso necesario para realizar los procesos requeridos y no más.
- Ofuscación. Este procedimiento sirve para aislar por confusión, aturdimiento, obscurecimiento u ocultamiento de una penetración potencial en el sistema. Esto se podría hacer, ocultando algunos archivos que no sean desplegados en el listado de archivos, inhibir el despliegue de la entrada en el "user name" y en el "password".

Un procedimiento que ayuda a reducir la vulnerabilidad inherente en comunicación de datos es comunmente referida a una encriptación o criptografía. Los sistemas de encriptación comunes envuelven :

* Sustitución. El cual es la relocalización de mensajes de caracteres con otros caracteres por medio de tablas.
* Transformación. El cual es la conversión de caracteres en un mensaje por un procedimiento aritmético.
* Transposición. La cual cambia el orden de caracteres en un mensaje.

Se pueden instalar cajas de encriptación entre una terminal y el modem. El más común de los métodos es el de cambiar caracteres por letras y números en el mensaje original.

Identificación

Si un sistema instala procedimientos de aislamiento, entonces los sistemas deben tener también, la habilidad para identificar interfases autorizadas y apropiadas. El sistema debe tener la habilidad de distinguir entre aquellos usuarios que su acceso es permisible y aquellos quienes no lo tienen. Dependiendo en el nivel de seguridad requerido, ya sea la persona, la terminal, el archivo, y/o el programa deben ser identificados, para que el derecho de uso pueda ser verificado, y el usuario pueda ser contablemente autorizado. Los métodos para efectuar esta identificación son los siguientes :

- Poseción de usuario. Un usuario es identificado por algo que el tiene en su posesión. Los puntos de identificación pueden consistir de:

  * Códigos (también llamados passwords)
  * Claves para asegurar
  * Gafetes
  * Cintas magnéticas o tarjetas ópticas

* Números telefónicos
* Número de terminal
* Claves de encripción

La principal desventaja de estos puntos de identificación es que la probabilidad es relativamente alta de que ellos puedan obtener estos puntos y usarlos en su contra.

- Algún usuario conoce. Un usuario es identificado sobre la base de que él sabe algo y solo él lo conoce. Ejemplos de estos puntos son:

  * Códigos personalizados que son cambiados regularmente.
  * Secuencias donde las respuestas del usuario son un conjunto predispuesto de preguntas, por ejemplo, dirección anterior, lugar de nacimiento, color de los ojos de la esposa, etc., La efectividad de este punto de identificación está directamente relacionada al rango de cambio.

- Características del usuario. El usuario es identificado sobre la base de que algo es parte de él y únicamente suyo. Estas características pueden dividirse en dos categorías:
  * Neuromulscular, tal como una firma y escritura.
  * Genética. La categoría de genética cubre lo siguiente: -Geometría del cuerpo (identificación de la geometría de la mano está siendo utilizado en muchos casos)
    - Huellas digitales
    - Patrones de respuesta de voz
    - Apariencia facial (el uso primario está en el gafete, no está todavía disponible comercialmente para identificación por computadora).

- Iris del ojo y retina
- Impresiones del labio
- Patrones de onda del cerebro

Las características arriba mencionadas son características especiales que distinguen a una persona de otra. Sin embargo, la tecnología de cómputo no está disponible comercialmente para esta clase de identificaciones aún.

Posición de terminales. Sobre la base de posición, las terminales pueden ser dadas en diferentes clasificaciones y niveles de seguridad.

Autorización

Una vez que una persona ha sido identificada como un usuario válido, viene la pregunta, que autoridad tiene?, esto es, que archivos en una base de datos los procedimientos deben ser arreglados para determinar quién tiene acceso a que archivos, quienes tienen el derecho de agregar y borrar, y quién es el responsable de administrar esos archivos. Los siguientes puntos ayudan a tratar el concepto de autorización.

- Categorizar la autorización. Este paso determina la autoridad específica de usuarios, programas y hardware. Las clases de autoridad pueden incluir usuarios para documentar, usuarios para equipar, usuarios para programar, usuarios para archivar, terminal para programar, programa para archivar, programa para programar, etc.

  Esas actividades que deben ser designadas en conjunción con tipos de autoridad son leídas, escritas, agregadas, cambiadas, borradas, copiadas, creadas y apendizadas, etc.

- Uso de códigos. Los códigos (también llamados claves) son ligados a una tabla de autorizaciones. La tabla de autorizaciones es turnada a una tabla de identificaciones, esto es, el usuario es identificado primero como válido. Entonces esto determina que puede hacer el usuario. Aún más, los códigos pueden ser asignados no solamente a archivos sino que pueden llegar a nivel de registro y si es necesario a campos.

- Programa de seguridad. El centro de cómputo por sí mismo debe ser programado no solamente para identificar usuarios válidos sino asegurarse que la autoridad apropiada ha sido otorgada.

  En suma, el programa de seguridad debe tener la habilidad de cambiar la identificación y autorización también como los cambios en los requerimientos de seguridad basados en la hora del día, día de la semana, fines de semana, días festivos, etc. Por ejemplo, ciertos usuarios deberían perder su autoridad en fines de semana, vacaciones, o días festivos. Incluído en el programa, debe también tener una rutina que reporte la fuente de cualquier violación intentada inmediatamente.

Autenticidad

Los procedimientos de autenticidad son requeridos para mostrar que algo es válido o genuino.

Aunque alguna o algunas facilidades pueden ser identificadas apropiadamente y autoridad dada para accesar algo o para realizar alguna actividad, el sistema no puede asegurar que el usuario es válido especialmente si el usuario es identificado sobre la base de "que tiene" o "que conoce".

Periódicamente, durante la utilización de archivos sensitivos (también como otros recursos), la validación de los usuarios debe ser confirmada. Esta confirmación puede incluir uno o todos los procedimientos de autenticidad siguientes:

- Observación física; enviar a alguien a la fuente de emisión para confirmar que el usuario es quien lo está reclamando.

- Desconexiones periódicas y procedimientos de volver a llamar, por ejemplo, una terminal es desconectada y conectada nuevamente para ver si la terminal apropiada responde.
- Solicitudes periódicas para mayor información o reverificación del usuario.

Monitoreo

Monitoreo es el hecho de observar, checar o vigilar algo. Este concepto reconoce que más tarde o más temprano, o en forma accidental o intencional, los controles ya mencionados serán neutralizados o rotos. Algunas capacidades del sistema específicos soportan los procedimientos de monitoreo incluyendo lo siguiente :

- Detección de violaciones de seguridad; un sistema de seguridad debe ser instalado para detectar cualquier violación de seguridad tan pronto como éste ocurra. Ejemplos de violaciones son, desuniones de usuarios de códigos de identificaciones de terminal, y solicitudes no autorizadas para un archivo.

CAPITULO IV

INTRODUCCION

La planeación de una metodología estandarizada para auditar sistemas de información computarizados en operación tiene como objetivo dar un enfoque sistemático que permita al Auditor en Sistemas de Información realizar su actividad con mayor eficiencia y efectividad.

El avance de nuevas tecnologías y la necesidad de automatizar procedimientos, impone necesidades de prever los diversos tipos de riesgos existentes. La oportunidad de establecer controles y supervisarlos, no solo resuelve la necesidad de supervisar las actividades, sino garantizar la medida de la obtención de resultados con alta eficiencia.

La auditoría establece las acciones pertinentes para evaluar los diversos tipos de riesgos, catalogando su grado de incidencia y su probabilidad de ocurrencia, y planteará los controles pertinentes a aplicar. De la observación de estos controles y su evaluación, apoyándose en procedimientos de verificación y comprobación podrá emitir su opinión que retroalimentará al sistema, pudiéndose establecer un seguimiento integral. El planteamiento metodológico se descibirá posteriormente.

La metodología propuesta en este capítulo no es la única para fines específicos, sin embargo es una alternativa para establecer un enfoque sistemático al proceso de auditar un sistema de información en operación.

4. METODOLOGIA PARA EVALUAR UN SISTEMA DE INFORMACION COMPUTARIZADO EN OPERACIÓN

4.1. METODOLOGIA ESTANDARIZADA DE AUDITORIA INFORMATICA

El Auditor en Sistemas de Información (ASI) debe entender los pasos y técnicas necesarias para planear, desempeñar y completar una auditoría, apegándose en todo momento a las normas, y al uso adecuado de procedimientos y técnicas comunes en el desarrollo de auditorías.

* Planear un enfoque de auditoría eficiente y efectivo, definiendo los objetivos y el alcance de la auditoría, preparando el programa de la auditoria y planaendo los recursos necesarios.

* Obtener y documentar las pruebas de auditoría, utilizando las técnicas apropiadas,

* Evaluar y presentar un informe de hallazgos, conclusiones y recomendaciones para informar de su efectividad, eficiencia y el estado de los controles,

* Evaluar las acciones tomadas por la administración con respecto a la implantación de las recomendaciones contenidas en el informe de auditoría.

4.2. PLANEACION ESTRATEGICA

La planeación adecuada es el primer paso en la realización efectiva de las auditorías informáticas.

El Auditor deberá entender el entorno general de la empresa, donde la auditoria va a ser realizada, así como los riesgos de control y los riesgos de la empresa asociados.

Las siguientes son parte de las áreas que deberán ser cubiertas durante la planeación de la auditoria :

4.2.1. Entender la Empresa y su Medio Ambiente

Al plantear la auditoria, el auditor deberá tener una comprensión general del medio ambiente bajo revisión. La auditoría deberá incluir un entendimiento general de las diversas actividades de la empresa y funciones referentes al tema de auditoria. El auditor necesita entender el entorno regulador en el cual opera la empresa.

Los pasos a seguir por el auditor para obtener una comprensión de la empresa debe incluir :

* Estudiar cualquier informe
* Leer materiales retrospectivos, incluyendo publicaciones, informes anuales, pre-informes de análisis financieros entre otros.
* Entrevistar a los directores principales para entender las actividades de la empresa.
* Revisar previamente los informes de auditoria y los planes estratégicos a corto y largo plazo.
* Conocer material sobre el comité de sistemas.

Riesgos de Auditoría y Materialidad.

El riesgo de Auditoría puede ser definido como el riesgo de que la información/informe financiero puede contener un error material o que el Auditor no pueda detectar un error que ya haya ocurrido. El riesgo de Auditoria se divide en :

* Riesgo Inherente. Un error puede ser material o significativo cuando se combina con otros encontrados durante la auditoría, asumiendo que no hay controles compensatorios relacionados.

* Riesgo de Control. Un error material no será evitado o detectado oportunamente con base en un sistema de controles internos.

* Riesgo de Detección. Es el riesgo que un auditor tiene al realizar pruebas exitosas de un procedimiento de análisis inadecuado. El auditor puede concluír que no existen errores materiales cuando en realidad los hay.

La palabra "material", asociada con cada uno de estos componentes o riesgos, se refiere a un error que debería ser considerado significativo cuando se realiza una auditoría. Para una auditoría financiera, un error material podría ser uno que afecta los estados financieros. En una Auditoría de Sistemas de Información Computarizados, la definición de un error material dependerá del tamaño o importancia de la entidad bajo auditoria, así como de otros factores.

* Entrevistar al personal responsable del área de sistemas para entender y documentar el ambiente general del centro de cómputo en cuanto a su estructura organizacional y plataformas de hardware y software.

Riesgo de la Empresa.

Los riesgos de la empresa son aquellos que pueden impactar a largo plazo en la factibilidad de un negocio o compañía.

Objetivos de Control Interno.

Un sistema automatizado bien diseñado deberá tener controles internos sobre todo en sus principales funciones. Además el ASI entenderá los objetivos de control básicos que deberán existir para todas las aplicaciones. Los objetivos del sistema de control interno incluyen :

* Controles Contables Internos. Son principalmente dirigidos a las operaciones contables. Esto significa el respaldo de los valores y la recuperación de los registros financieros.

* Controles Operacionales. Son establecidos para vigilar que las funciones y actividades / día cumplan con los objetivos de la empresa.

* Controles Administrativos. Son establecidos de acuerdo con la eficiencia operacional en el área funcional. Los controles administrativos pueden ser descritos como soporte de los controles operacionales.

Algunos ejemplos de controles internos son :

* Salvaguarda de activos.
* Estar de acuerdo con las políticas corporativas o requerimientos legales.
* Exactitud y cumplimiento de transacciones.
* Recuperación de los procesos.

Objetivos de Control en los Sistemas de Información.

Los objetivos de control interno aplicados a todas las áreas, podrían ser manuales o automatizados. Por lo tanto, el ASI debería tomar los objetivos de control interno y trasladarlos hacia procedimientos específicos de auditoría en sistemas de información.

Algunos ejemplos de objetivos de control interno automatizados incluyen :

* Transacciones capturadas y actualizadas solo una vez.
* Las transacciones reprocesadas son reportadas.
* Las transacciones duplicadas son reportadas.
* Los archivos son debidamente respaldados para permitir una recuperación adecuada.
* Todos los cambios a la operación del software deben ser aprobados y evaluados.

Objetivos de Auditoría General.

La administración puede dar al ASI un objetivo general a seguir cuando se realiza la auditoría.

Por ejemplo, ellos pueden pedir al auditor que evalúe todos los controles internos de una área dada o pueden pedir que el auditor determine que el inventario de la localidad está en "buen estado".

En el primer caso, el ASI puede hacer una revisión general que consiste en observaciones, entrevistas y revisión de documentación. Puede no ser una evaluación detallada. En el caso posterior, el auditor puede realizar pruebas detalladas del inventario incluyendo prueba de cuentas y conciliaciones contables.

Entender los objetivos de la auditoría en general es un paso importante en la planeación de una auditoría en sistemas de información.

Objetivos de la Auditoria de los Sistemas de Información.

Un elemento clave en la planeación de una auditoría en sistemas de información consiste en trasladar los objetivos básicos de la auditoría a objetivos específicos de auditoría de sistemas de información.

El ASI deberá tener un entendimiento general de como los objetivos de la auditoría general pueden ser trasladados a objetivos específicos en el control de sistemas de información.

Procedimientos de Control General.

Los controles generales son sobre todo interdependientes y se aplican a todas las áreas de la organización. Los procedimientos de control incluyen políticas y procedimientos establecidos por la administración, para proporcionar una razonable seguridad sobre los objetivos específicos que se llevarán a cabo. Los siguientes son los procedimientos de control :

* Políticas de seguridad lógica, organizacional y procedimientos para asegurar una adecuada autorización de transacciones y actividades.
* Políticas globales para el diseño y uso de documentos adecuados de registros, a fin de ayudar a asegurar el registro adecuado de transacciones (ejem. rastro de auditoría de transacciones).
* Procedimientos y características para asegurar los respaldos adecuados de acceso, y uso de valores y facilidades.
* Políticas de seguridad física que se apliquen a todos los centros de cómputo.

Esta lista puede ser aumentada, sin embargo, el ASI deberá entender éstos conceptos de procedimientos de control general y cómo serán aplicados en la planeación de una auditoría.

Los controles son generalmente clasificados en :

* Preventivos.

Son aquellos controles que están diseñados para prevenir la ocurrencia de un error, omisión o acto malicioso. Un ejemplo de control preventivo, sería el uso de software de control de acceso que permite sólo al personal autorizado la entrada a archivos importantes.

* Correctivos.

Son aquellos controles que corrigen los errores, omisiones, o actos maliciosos, una vez que se han detectado. Un ejemplo de un control correctivo, es un proceso automatizado que compruebe la captura de fechas de facturas y por omisión dé la fecha del sistema para facturas que tienen datos que se salen del rango checado por este campo.

* Detectivos.

Son aquellos controles que detectan un error, omisión o acto malicioso que ha ocurrido y se ha reportado. Un ejemplo de un control detectivo, sería la impresión de la clave común de acceso violada.

Procedimientos de Control en Sistemas de Información.

Cada procedimiento de control general puede ser trasladado a un control específico de sistemas de información.

Por ejemplo, el ASI puede trasladar su procedimiento general de un respaldo a un sistema de información, relacionado con un grupo de procedimientos de control que cubren los respaldos de acceso en programas de computadora, datos y equipo de cómputo.

Los procedimientos de control de información pueden ser agrupados en las siguientes áreas :

* Procedimientos de control de organización general.
* Accesos a los datos y programas.
* Metodologías en el deasarrollo de sistemas.
* Operaciones de procesamiento de datos.
* Programación de sistemas y funciones de soporte técnico.
* Procedimientos de aseguración de calidad del procesamiento de datos.

El ASI entenderá cómo los procedimientos de control general pueden ser trasladados a otros más específicos de control de sistemas de información. Este entendimiento es importante en la planeación de una auditoria. El concepto del Debido Cuidado Profesional es también fundamental en la planeación de una auditoría. El Debido Cuidado Profesional es la Norma General No. 8 para la realización de un trabajo. Esta norma establece : "El Debido Cuidado Profesional debe ser efectuado en todos los aspectos del trabajo del Auditor, incluyendo la observación aplicable a las normas de auditoría."

Procedimientos de Auditoría General.

Los procedimientos de Auditoría General son las etapas básicas en la realización de una auditoría e incluyen lo siguiente :

* Evaluación de riesgos,
* Planeación de auditoría individual,
* Revisión preliminar del área / o sujeto de auditoría,
* Obtener, registrar y entender el área / o sujeto de auditoría,
* Evaluar el área / sujeto de auditoría,
* Prueba de cumplimiento,
* Prueba sustantiva,
* Reporte de Auditoría, y
* Seguimiento.

Procedimiento de Auditoría en Sistemas de Información.

Las auditorías de los sistemas de información siguen los mismos procedimientos generales recomendados anteriormente. Por ejemplo, el primer paso de la planeación de la auditoría es obtener un entendimiento general del área a auditar.

Por lo tanto el auditor entenderá los procedimientos de pruebas y evaluación de los controles de los sistemas de información, estos procedimientos incluyen :

* El uso de software generalizado de auditoría para examinar los contenidos de los archivos de datos.

* Técnicas de diagramas de flujo para documentar aplicaciones automatizadas.

El ASI debe tener suficiente entendimiento de estos y otros procedimientos para permitir la planeación de prueba de auditoría apropiada.

Otros Criterios de Planeación y Consideración.

El resultado de los negocios, requerimiento regulatorio y otras materias afectarán el proceso de planeación del ASI. El ASI deberá entender que otras consideraciones pueden impactar el rendimiento general de la auditoría y tomará en consideración lo siguiente :

* La implantación de sistemas / fin del mismo.

* Actual y futuras tecnologías.

* Limitación de los recursos de los Sistemas de Información.

Crímenes por Computadora.

Cuando oimos hablar de delitos por computadora pensamos que es algo probable que ocurra en nuestro medio, sin embargo, debemos observar dos puntos importantes :

* 1 - La seguridad de los sistemas ha descansado en "controles por ignorancia", es decir, como la mayoría de la gente anteriormente no conocían nada de computadoras, no podían alterar mal intencionalmente los sistemas o la información en ellos contenida. Pero estos "controles por ignorancia" serán más débiles conforme aumenta la gente con mayor conocimiento de aspectos computacionales.

* 2 - El incremento de las redes computacionales, la complejidad de los sistemas y el creciente intercambio de información hacen más amplio el número de personas que pueden accesar un sistema, y por consiguiente, deben existir más y mejores controles para incrementar la seguridad.

Los sistemas de claves de acceso (passwords), deben ser más efectivos, permitiendo el acceso del usuario sólo a las aplicaciones o archivos que son necesarios para su trabajo y no a todo el sistema. Será necesario tener controles y registros para identificar las transacciones que cada usuario haga en un sistema, para prevenir los ambientes de anonimato donde el usuario siente que nadie puede darse cuenta de lo que hace, lo cual invita a los delitos o a las ineficiencias.

Categorías de Delitos por Computadora.

Los delitos por computadora pueden ser diversos, pero básicamente se refieren a acciones en contra del equipo de cómputo y / o software relacionado con él.

Existe el "Acta Federal de Protección a los Sistemas de Cómputo" donde se definen cuatro categorías principales de delitos por computadora :

* 1 - Introducción de datos fraudulentos en un computador.

* 2 - Uso no autorizado de un computador y sus facilidades.

* 3 - Alteración o destrucción de la información.

* 4 - Robo por medios electrónicos, de dinero, herramientas financieras, servicios o información.

Métodos de Ejecución de Delitos

Los métodos que se utilizan para cometer estos delitos son muy variados :

Entre los más comunes se encuentran el de la alteración de datos de entrada, el cual puede ser utilizado en contra de sistemas de nóminas, cuentas por cobrar, cuentas por pagor y/o proveedores, etc.

Si no se cuenta con un control adecuado de autorizaciones y separación de funciones, este método puede ser fácilmente implementado por cualquier operador o persona con acceso al sistema.

Otro método es conocido como la "Técnica de Salami" que consiste en llevar pequeñas "rebanadas" de dinero, casi indetectables, de muchas cuentas a una sola cuenta, a la que el perpetrador tiene acceso.

Algunos métodos como el del "Caballo de Troya", "Bombas Lógicas", etc, atenta con la integridad de los programas y la información y cuando incluyen la característica de reproducirse asi mismos, reciben el nombre genérico de "Virus". Los virus son tema para mucha discusión y análisis; aquí sólo diremos que al igual que en los casos de los virus biológicos, la mejor manera de evitar su propagación y contagio, es seguir reglas de "higiene" básicas, no intercambiando diskettes sin control, evitando las copias no autorizadas, revisando periodicamente los sistemas con los programas de diagnósticos de virus que ya existen en el mercado y por si acaso, contando siempre con los respaldos adecuados para la información y programas.

Reglamentaciones

Dentro de los esfuerzos de índole legal para evitar o castigar los delitos por computadora se creó el Acta sobre Abusos y Fraudes con Computadoras, la cual establece penas de multas considerables y prisión, para aquellos que conscientemente accesan a un computador sin autorización y obtengan ganancias por los movimientos fraudulentos.

Esta Acta ha tenido algunas revisiones y contiene otras penas para violaciones que no necesariamente le brinden una ganancia al perpetrador del delito.

En cuanto a la prevención de copias de programas existe el Acta de Derechos de Autor de Software de Computadoras, lo cual provee a los desarrolladores de programas de Derechos exclusivos sobre sus productos y pueden ser un instrumento muy eficaz para enfrentar la piratería. Finalmente, podemos afirmar que si bien es mucho lo que falta por clarificar respecto a los delitos computacionales; es por eso que se deben establecer controles, políticas y procedimientos, que coadyuven a preservar la integridad y buen uso de los activos informáticos.

El ASI tiene la responsabilidad de identificar y reportar crímenes por computadora cuando son detectados en una auditoría típica de sistemas de información. El ASI debe tener un entendimiento general de la naturaleza de los crímenes por computadora y de áreas que son vulnerables a estas actividades. Este entendimiento ayudará al ASI a planear la auditoría con esos riesgos potenciales en mente.

4.3. DESARROLLO DE PROGRAMAS DE AUDITORIA

4.3.1. Estructura y Fases del Programa de Auditoría.

Un programa de auditoría es un grupo de procedimientos de auditoría documentados, diseñados para llevar a cabo los objetivos de auditoría planeados. Un programa de auditoría debe incluir lo siguiente :

*** Sujeto de Auditoría**

- Identificar el área a auditar.

*** Objetivo de la auditoría**

- Identificar el próposito de la auditoría. Por ejemplo, un objetivo puede ser determinar qué cambios pueden ocurrir en el código fuente en un programa de un medio ambiente bien definido y controlado.

*** Ambito de la auditoría**

- Identificar los sistemas específicos ó la unidad de la organización a ser incluida en la revisión. Por ejemplo, en los cambios del programa del ejemplo anterior, el ámbito puede estar limitado a la revisión de un sólo sistema de aplicación o a un periodo de tiempo limitado.

*** Planeación de una auditoría**

- Identificar las herramientas, técnicas y recursos requeridos,

- Identificar las fuentes de información para evaluar y revisar aspectos tales como; diagramas funcionales de flujo, políticas, normas, procedimientos y papeles de trabajo anteriores a la auditoría.

- Identificar centros de cómputo para ser auditados.

Procedimientos y pasos de auditoría :

- Reunir datos,

- Identificar y seleccionar vías de acceso de auditoría para la verificación de controles.

- Identificar y obtener las políticas, normas y lineamientos a analizar.

- Desarrollar herramientas y metodologías de auditoría para evaluar y verificar los controles.

* Procedimientos para examinar los resultados de pruebas ó análisis.

* Procedimientos para comunicación con la administración.

* Preparación del informe de auditoría.

* Procedimientos de análisis del seguimiento.

- Normas para evaluar / examinar la eficiencia y efectividad.

- Procedimientos para examinar controles.

- Revisar y evaluar la validez de documentos, políticas y procedimientos.

El programa de auditoría también se convierte en una guía para documentar los pasos de la auditoría realizada y señalar el lugar de la evidencia en los papeles de trabajo de la misma. El ASI debe firmar y fechar los diversos pasos, tal como los realiza para proporcionar una pista de registro y realización.:

Aunque un programa de auditoría no sigue necesariamente un grupo de pasos, el ASI seguiría típicamente las fases del programa secuencial para obtener una comprensión de la entidad bajo auditoría, evaluar la estructura de control, y entonces examinar los controles.

4.3.2. Prueba de Cumplimiento vs. Prueba Sustantiva.

La diferencia entre la prueba de cumplimiento y la prueba sustantiva es un concepto importante para el ASI. Una prueba de cumplimiento determina si los controles

están siendo aplicados, en la manera escrita en la documentación del programa o como se describe por el auditado. Una prueba de cumplimiento determina si los controles están siendo aplicados de una manera que "CUMPLA CON" las políticas y procedimientos de la administración. Por ejemplo, si el ASI está preocupado de que los controles de la biblioteca de programas están trabajando adecuadamente, puede seleccionar una muestra de programas para determinar las versiones fuente y objeto de las mismas.

Una prueba sustantiva establece la suficiencia de los controles existentes en proteger a la organización de actividad fraudulenta. Los auditores financieros usarían pruebas sustantivas para examinar los errores monetarios que han afectado directamente los balances de declaración financiera.

Para un ASI, una prueba sustantiva es mucho más extensa. Un auditor puede desarrollar una pureba sustantiva para determinar si los registros del inventario de la biblioteca de cintas están operando correctamente.

Para realizar esta prueba puede tomar el 100% del inventario o puede usar una muestra estadística, la cual permitirá al auditor desarrollar una conclusión con respecto a la precisión del inventario completo.

4.3.3. Controles Clave

Un propósito básico de cualquier auditoría de sistemas de información, consiste en identificar los controles clave y realizar los procedimientos de auditoría para examinarlos.

Generalmente, no resulta eficiente tratar de evaluar todos los controles, por lo tanto, los programas de auditoría deben estar diseñados para enfocarse a identificar y evaluar los controles claves.

4.3.4. Reglas de Evidencias

La evidencia es cualquier información usada por el ASI para determinar si la entidad o los datos que están siendo auditados, siguen criterios u objetivos de auditoría establecidos. La evidencia de auditoría puede incluir observaciones del Auditor, notas tomadas en entrevista, material extraído de la documentación correspondiente o interna , o de resultados de procedimientos de prueba de auditoría.

Mientras toda la evidencia ayudará al ASI a desarrollar las conclusiones de auditoría, alguna evidencia es más confiable que otras. Las determinantes para evaluar la confiabilidad de la evidencia de auditoría incluyen :

* La independencia del "proveedor"de la evidencia

La evidencia obtenida de fuentes exteriores es más confiable que la obtenida dentro de la organización.

Esta es la razón por la cual los auditores externos mandan cartas de confirmación para la verificación de cuentas por cobrar.

* Capacidades de la persona que proporciona la información o evidencia.

La evidencia objetiva es mucho mejor ya que la subjetiva requiere una interpretación. Un cálculo de un fondo en efectivo por un Auditor Financiero es evidencia directa, objetiva.

Un análisis de eficiencia de una aplicación de un ASI, basada en discusiones con cierto personal, puede no ser evidencia.

Una comprensión de las reglas de evidencia es importante para el ASI, quien puede tener una diversidad de tipos de evidencia.

4.4. PLANEACION DE RECURSOS DE AUDITORIA

Los ASI son un recurso limitado en muchas organizaciones, el tiempo en sus revisiones debe ser planeado y programado adecuadamente. El ASI debe entender las técnicas para dirigir proyectos de auditoría con miembros del equipo de auditoría apropiadamente entrenados.

Las habilidades y el conocimiento deben ser tomados en consideración cuando se planeen auditorías y se asigne al equipo tareas de auditoría específicas.

4.4.1. Recursos de Personal

Los Directores de Auditoría en Sistemas de Información, deben tener un conocimiento de los recursos que están disponibles dentro de una organización, para realizar auditorías. Los ASI pueden contar con diversos antecedentes, incluyendo programadores, auditores financieros, y licenciados en varios grados de experiencia, auditores certificados (CISA).

Los directivos deben de tener una comprensión de los recursos disponibles dentro de la organización para permitirles realizar apropiadamente las auditorías de sistemas de información.

4.4.2. Restricciones en la Conducción de una Auditoría

Aunque una organización de auditoria puede estar dotada con personal que posee una mezcla apropiada de las habilidades requeridas, las restricciones pueden limitar la disponibilidad de su personal.

Por ejemplo, los ASI pueden ser solicitados para apoyar a los auditores financieros con procedimientos asistidos por computadora al final del año, así, esos auditores en sistemas de información pueden no estar disponibles durante este periodo para otros proyectos de auditoria.

Para entender estas restricciones en la conducta de una auditoría dada, los ASI deben tener una buena comprensión de las técnicas globales de administración de proyecto.

4.4.3. Técnicas de Administración del Proyecto

Han sido desarrolladas numerosas técnicas de administración de proyectos que pueden ser comparadas para administrar proyectos de auditoria.

Algunas son automatizadas y otras son manuales. Todas ellas incorporan los siguientes pasos básicos :

*** Desarrollar un plan detallado**

El plan debe distribuir los pasos de auditoría necesarios a través de una línea de tiempo. Deben hacerse estimaciones realistas de el tiempo requerido para cada tarea de auditoría dado la debida consideración a la disponibilidad de los auditados.

*** Reporte de la actividad del proyecto en contra del plan.**

Debe haber algún tipo de sistema de reporte establecido tal, que los ASI puedan reportar su progreso actual en contra de los pasos de auditoría planeados.

*** Ajustar el plan y tomar acciones correctivas cuando se requieran.**

Los logros reales deben ser medidos contra el plan establecido sobre una base continua. Cambios a las asignaciones del ASI o a programas planeados, deben realizarse cuando se requieran.

4.4.4. Relacionar los Recursos Disponibles con los Requerimientos

Un componente básico de una buena planeación es la relación de los recursos de auditoría disponibles con las tareas definidas en plan de auditoría. Este es frecuentemente un delicado trabajo de balanceo para el ASI al preparar el plan. Habrá una mezcla de habilidades que deben ser balanceadas contra los requerimientos del proyecto de auditoría.

4.4.5. Definir, Organizar y Monitorear Tareas de Auditoría

Las labores de administración del proyecto generalmente siguen las tareas de administración discutidos brevemente. El ASI debe seguir buenas técnicas de administración al analizar el progreso de los proyectos de auditoría de sistemas de información.

4.4.6. Capacitación de Personal

La tecnología en los sistemas de información está cambiando constantemente. La capacitación debe mantener la competencia individual del ASI a través de la actualización de las técnicas existentes.

Para ayudar en la comprensión de esta área, el ASI debe estar familiarizado con los requerimientos de capacitación constante para continuar con la certificación CISA.

4.5. TECNICAS DE OBTENCION DE EVIDENCIA

La obtención de evidencia es un paso clave en el proceso de auditoría. El ASI debe estar consciente de las diversas formas de evidencia de auditoría y como pueden ser resumidas y analizadas.

El ASI entenderá la norma general No. 7 de la EDPAF, "Obtención de Evidencia" y obtendrá evidencia de una naturaleza y suficiencia para apoyar los hallazgos de auditoría.

4.5.1. Análisis de las Estructuras de Organización de los Sistemas de Información

Un fuerte plan de organización con una adecuada segregación de tareas es un control general clave en una función de sistemas de información.

El ASI debe entender los controles organizacionales generales y poder evaluarlos en la organización bajo auditoría.

4.5.2. Analizar las Normas de Documentación de los Sistemas de Información

Un primer paso en el análisis de la documentación de un sistema de información es entender las normas de documentación establecidas dentro de la organización. El ASI buscará un nivel mínimo de documentación de los sistemas de información que pueden incluir:

* Documentos de inicialización del desarrollo de sistemas,
* Especificación del diseño funcional,
* Historia de cambios de programa, y
* Manuales de documentación a usuario

Los ASI reconocen que en las técnicas de desarrollo de sistemas tales como CASE, (Computer Assisted Software Enginering) la documentación tradicional de los sistemas no será requerida ó será en forma automatizada más que sobre papel. Sin embargo el ASI debe buscar normas y prácticas de documentación dentro de la organización de los sistemas de información.

4.5.3. Analizar la Documentación de los Sistemas

El ASI podrá analizar la documentación de un sistema dado y determinar si sigue las normas de documentación de la organización. Además, el ASI debe de entender el enfoque más reciente para desarrollar sistemas, tales como CASE ó PROTOTIPO; como se constituye la documentación.

El auditor reconocerá otros componentes de la documentación de los sistemas de información tales como especificaciones de base de datos, descripción de archivos o listados de programas autodocumentados.

4.5.4. Entrevistar al Personal Apropiado

Aunque la literatura en auditoría de sistemas de información no enfatice las técnicas de entrevistas en auditoría, ésta es una habilidad importante para el ASI. Las entrevistas de auditoría deben estar organizadas por adelantado, seguir una linea fija, y ser documentada a través de notas de entrevistas. Una forma o listado de control de entrevista del auditor es un buen acercamiento. El auditor siempre se dará cuenta que el propósito de tales entrevistas es obtener evidencia de auditoría. Las entrevistas al personal son descubrimientos, normalmente, y nunca deben ser acusadoras.

4.5.5. Observar el Funcionamiento de Operaciones y Empleados

La observación de operaciones es una técnica de auditoría clave para muchos tipos de análisis.

El ASI debe ser objetivo mientras hace observaciones y debe documentar todo con suficiente detalle para poder presentarlo como evidencia en una fecha posterior, si es requerido.

4.5.6. Utilización de Cuestionarios y Diagramas de Flujo como Herramienta para Auditar Aplicaciones

Una herramienta de auditoría es ayuda tangible que asiste al ASI en la implementación de una técnica de auditoría.

A continuación se presentan las principales herramientas utilizadas y recomendadas como apoyo para el auditor en informática en el desempeño de sus funciones.

* Aplicación de Cuestionarios

* Diseño de diagramas de flujo

4.5.7. Técnicas de Documentación de Auditoria.

El ASI debe entender las técnicas para documentar un sistema de información, además de documentar la comprensión del ambiente de los sistemas de información. El ASI puede preparar diagramas de flujo de los sistemas adecuados y entendibles.

Seleccionar y Examinar Controles Clave

El análisis inicial de un sistema de información de un ASI debe identificar los controles clave. El ASI entonces decidirá examinar estos controles a través de los métodos de verificación sustantiva y de cumplimiento.

El auditor debe identificar los controles de aplicación clave, después de desarrollar una comprensión y documentar la aplicación. Basado en esa comprensión, el auditor identificará los puntos de control clave en la aplicación.

La identificación permitirá al auditor desarrollar una comprensión preliminar a través de purebas de cumplimiento de aquellos controles para determinar si están trabajando como se desea. Los resultados de estas pruebas de cumplimiento permitirán al auditor diseñar pruebas de cumplimiento o sustantivas más extensivas.

4.5.8. Aplicar Técnicas de Muestreo

El ASI debe tener un profundo entendimiento de las técnicas de muestreo de auditoría, incluyendo procedimientos de muestreo de atributos no estadísticos o de variables y estadísticos. El auditor sabra aplicar el tipo apropiado de pruebas de muestreo para las pruebas de auditoría sustantiva y de cumplimiento.

* Muestreo de atributos

También conocido como muestra de estimación de frecuencia, es la técnica para estimar la tasa de ocurrencia de un control dado. Un grupo de controles relacionados (los atributos). Un ejemplo de un atributo que puede ser examinado son las aprobaciones firmadas en las formas de solicitud de acceso a la computadora.

* Muestreo de variables

También conocido como estimación monetaria o muestreo de estimación promedio, es la técnica usada para estimar el valor monetario de alguna otra unidad de medida, tal como peso, de una población en una porción de la muestra. Esta técnica es también usada para predecir el valor monetario de los errores contenidos en una población dada.

Un ejemplo de muestreo de variables sería estimar el número de módulos de código objeto obsoletos, basado en una evaluación de muestra de la biblioteca de código objeto de producción.

Los elementos clave en una prueba de muestreo de auditoría incluyen:

* Determinar los objetivos de la prueba

*Definir la población para ser muestreada

* Elegir una técnica de muestreo

* Realizar un plan de muestreo

* Evaluar los resultados de la muestra

4.5.9. Técnicas de Auditorías Asistidas por Computadora (TAAC)

El ASI debe tener un profundo conocimiento de las técnicas asistidas por computadora y dónde deben ser aplicadas. Este entendimiento debe incluir el uso de software generalizado de auditoría y técnicas más avanzadas, tal como generadores de datos de prueba y técnicas de facilidad de pruebas integradas.

Además de seleccionar la técnica apropiada, el auditor debe entender la importancia de documentar los resultados de tales pruebas para propósito de evidencia de auditoría.

Ejemplos del uso de técnicas TAAC son las siguientes :

* Usar un generador de datos de prueba para preparar prueba de seguimiento, la lógica de programas de aplicación.

* Usar sistemas expertos que estén residentes en la computadora y llamen a analizar a módulos de software dentro del sistema operativo o del sistema de seguridad.

* Usar utilerías estándar residentes en los paquetes de software que especifiquen el estado de los parámetros usados para instalar el paquete.

* Usar los paquetes de biblioteca de software para verificar la integridad y la conveniencia de los cambios al programa.

4.6. EVALUACION DE LAS FORTALEZAS Y DEBILIDADES DE LA AUDITORIA

Después de desarrollar un programa de auditoría y de reunir evidencia de la misma, el siguiente paso es evaluar la información reunida para desarrollar una opinión de auditoría. Esto requiere al auditor considerar una serie de fortalezas y debilidades y entonces desarrollar varias opiniones y recomendaciones de auditoría.

Mientras esto es aplicado durante todo el proceso de auditoría a los sistemas de información, la norma general del EDPAF No.8 "Debido cuidado profesional" es particularmente importante el evaluar las fortalezas y debilidades de la Auditoría.

Evaluar los Requerimientos de Control.

El ASI debe evaluar los resultados de la evidencia reunida, de conformidad con los requerimientos y objetivos de control establecidos durante la etapa de planeación; para esto es necesario tener una cantidad considerable de juicio, mientras los controles estén frecuentemente confusos. Una matriz de control es utilizada para evaluar el debido nivel de los controles.

La matriz trabaja colocando los tipos de errores conocidos que pueden ocurrir en el área bajo revisión en el eje superior y los controles conocidos o los errores corregidos en el eje lateral. Entonces usando un método de clasificación se llena la matriz con la medición apropiada. Cuando está completa, mostrará las áreas donde los controles son débiles o están ausentes.

4.6.1. Información Relevante y Periférica.

El auditor reune diversas evidencias durante la auditoria. Alguna puede ser relevante a los objetivos de la auditoria, mientras otra puede ser considerada como irrelevante. El auditor debe enfocarse a los objetivos globales del análisis y no a la naturaleza de la evidencia reunida. El buen juicio será aplicado para determinar qué material es exactamente apropiado para los objetivos de la auditoría y cuál no es específicamente relevante.

4.6.2. Considerar los Controles de Compensación y su Superposición.

Como parte del análisis a sistemas de Información, el auditor de sistemas de información puede descubrir una variedad de controles fuertes y débiles.

Todos deben ser considerados cuando se evalúe la estructura global del control. En algunas ocasiones el control fuerte puede compensar a un control débil en otra área. Por ejemplo, aun si el auditor encuentra debilidades en un reporte de errores de transacciones de sistemas, el auditor puede encontrar que un proceso detallado de balanceo manual sobre todas las transacciones, compensa la debilidad en el reporte de errores. El ASI debe estar consciente de compensar controles en áreas donde son identificados como débiles.

Los controles de superposición son similares a los de compensación. Un control de superposición puede realizar otro control adecuado. En el ejemplo anterior, si el auditor no encontró ninguna debilidad en el reporte de errores de transacciones y también encontró el proceso de controles de balanceo fuerte, puede concluir que éstos son controles superpuestos.

Como ejemplo de un control de compensación, el auditor puede encontrar que el sistema administrador de cintas en el centro de datos tiene una debilidad de control en algunos parámetros que son establecidos para desviar o ignorar las etiquetas escritas en los registros cabecera de la cinta. Esta es una debilidad de control, sin embargo, el auditor puede encontrar procedimientos muy fuertes de organización y de establecimiento de trabajo en el centro de datos tal, que sólo las cintas correctas pueden ser montadas. Si los controles sobre los procedimientos de establecimiento de trabajo son considerados como adecuados, el auditor puede concluir que este control compensa a la debilidad de control de los de etiquetación de cintas.

Mientras una situación de control compensatorio ocurre cuando uno más fuerte apoya a uno débil, los controles superpuestos son dos controles fuertes. Por ejemplo, un centro de procesamiento puede emplear un sistema de tarjetas clave, para controlar el acceso físico. Si hay también un guardia adentro de la puerta, el cual pide a los empleados mostrar su tarjeta o insignia llave, esto sería un control superpuesto. Cualquiera de los dos controles pueden ser adecuados para restringir el acceso y los dos se complementan.

4.6.3. Considerar las Interrelaciones de los Controles

El ASI realizará una variedad de procedimientos de prueba y evaluará cómo éstos se relacionan.

El auditor puede no encontrar que cada procedimeinto esté establecido, pero debe evaluar la totalidad del control, considerando las fortalezas y debilidades de los procedimientos de éste.

4.6.4. Determinar la Naturaleza de las Operaciones Efectivas y Eficientes

El auditor analizará la evidencia reunida durante la auditoria, para determinar si las operaciones estudiadas están bien controladas y son efectivas. Esta es también un área que requiere el juicio y experiencia del auditor.

El auditor debe evaluar las fortalezas y debilidades de los controles; y entonces determinar si son efectivos en cumplir los objetivos de control establecidos como parte del proceso de planeación de auditoria.

4.6.5. Técnicas para Analizar Evidencia

El auditor debe tener conocimiento de las técnicas para analizar la evidencia. Por ejemplo, el auditor puede desear analizar hallazgos basados en tendencias estadísticas, ya sea en términos de tasas globales durante un análisis o como comparaciones periodo a periodo. El análisis de regresión es otra herramienta poderosa para este tipo de análisis, el cual permite al auditor estudiar una variedad de datos aleatorios y determinar si representan una tendencia.

4.6.6. Juzgar la Importancia de los Hallazgos

El concepto de importancia es un asunto clave para presentar hallazgos decisivos en un reporte de auditoria a la administración.Una debilidad en los controles de seguridad de los accesos físicos de la computadora en un sitio de cómputo distribuido remoto puede ser importante para la administración de tal sitio, pero no ser necesariamente esencial para la alta administración en las oficinas principales.

El ASI debe siempre juzgar qué hallazgos son importantes para los diversos niveles de la administración y debe reportarlas como corresponde. Sin embargo, una buena regla es incluir más puntos que reportar muy pocos.

4.7. REPORTES DE AUDITORIA

Los reportes de auditoría son el producto final del auditor. Este es el vehículo que el auditor usa para reportar hallazgos y recomendaciones a la administración. El formato exacto de un reporte de auditoría variará en cada organización. Sin embargo, el auditor habilidoso entenderá los componentes básicos de un reporte de auditoría y cómo comunicar adecuadamente los hallazgos de auditoría a la administración. El auditor debe entender las normas generales de la EDPAF No. 9 "Reporte de Cobertura y Auditoría" y el No. 10 "Reporte de Hallazgos y Conclusiones".

4.7.1. Estructura y Contenido del Reporte

No hay un formato específico para un reporte de auditoría y las normas de auditoría de la organización generalmente dictan el formato. Sin embargo, los reportes de auditoría usualmente tienen la siguiente estructura y contenido :

* Introducción al reporte, incluyendo una declaración de los objetivos de la auditoría.

* El período cubierto

* Una declaración general sobre la naturaleza y extensión de los procedimientos de auditoría realizados

4.7.2. Criterios para la Inclusión de Hallazgos en los Reportes de Auditoría

La decisión de incluir o no hallazgos en un reporte de auditoría dependerá de la importancia de los mismos y el futuro destinatario del reporte de auditoría.

Un reporte de auditoría dirigido al Comité de Auditoría del Consejo de Directores, por ejemplo, no puede incluir hallazgos que son importantes a la administración local pero que tienen poca importancia de control a la organización global. La decisión de incluir varios niveles de reportes de auditoría, depende de los lineamientos proporcionados por la alta administración. Sin embargo, el auditor debe tomar la decisión final, segun su criterio y experiencia, qué incluir o excluir en el reporte de auditoría.

El auditor debe entender las normas generales de la EDPAF No. 1 y No. 2 sobre independencia.

4.7.3. Restricciones sobre Recomendaciones a Implantar

El ASI debe reconocer que la administración puede o no puede implantar todas las recomendaciones de auditoría inmediatamente. Otros factores pueden retrasar tales acciones, por ejemplo, el ASI puede recomendar cambios a un sistema de información que también está sufriendo cambios o mejoras.

El auditor no debe necesariamente esperar que los otros cambios sean suspendidos hasta que sus recomendaciones estén instaladas adecuadamente, ambas pueden ser instaladas juntas.

El auditor debe discutir las recomendaciones y cualquier fecha planeada de implantación durante el proceso de liberación del reporte de auditoría.

Si es apropiado, el ASI puede reportar a la alta administración sobre el progreso de la implementación de estas recomendaciones.

4.7.4. Importancia Relativa de las Debilidades

Un reporte de auditoría incluirá una variedad de hallazgos, algunos de los cuales pueden ser bastante importantes, mientras que otros son menores en naturaleza.

En el seguimiento del programa de la administración para implantar recomendaciones, el auditor debe considerar su relativa importancia.

4.7.5. Comunicar Resultados a la Administración y Comités de Auditoría

El auditor debe estar consciente de que su máxima responsabilidad es con la administración principal y con el Comité de Auditoría del Consejo de Directores. Mientras estos grupos generalmente reciben cópia de todos los reportes de auditoría, de vez en cuando el ASI encontrará asuntos que deberán ser corregidos inmediatamente.

El auditor debe sentirse libre para comunicar estos asuntos o preocupaciones a la administración. Un intento de la administración principal para negar el acceso al auditor limitaría la independencia de la función de auditoría.

4.7.6. Declaraciones de Opinión y Conclusiones

El reporte de auditoría debe incluir una declaración de opiniones con respecto a los hallazgos del auditor. Como está definido en las normas generales de EDPAF No. 10, el auditor debe también comunicar cualquier reserva o descripción con respecto a la auditoría.

Esta puede tomar la forma de que los controles o procedimientos examinados fueron encontrados adecuados ó inadecuados. El balance del reporte de auditoría apoyará esta conclusión, y la evidencia global reunida durante la auditoría proporcionará un mayor nivel de apoyo.

4.7.7. Técnicas de Presentación

El auditor frecuentemente será requerido para presentar los resultados del trabajo de auditoría a varios niveles de la administración.

El auditor debe tener un completo conocimiento de las técnicas de presentación necesarias para comunicar esos resultados, las técnicas de presentación pudieran incluir lo siguiente :

Un reporte fácil de leer, gramaticalmente correcto y conciso que presente los hallazgos a la administración. Muchos Directores Ejecutivos no están familiarizados con los términos de cómputo, por lo tanto, los reportes a la alta dirección deben estar libres de terminología técnica. Los complementos detallados pueden ser de naturaleza más técnica, ya que la administración de operaciones requerirá los detalles para corregir las situaciones reportadas.

* Transparencias generales ó diapositivas de 35 mm, generadas a través de paquetes de software de cómputo gráfico.

4.7.8. Acciones de la Administración para Implantar las Recomendaciones.

Los auditores deben darse cuenta que auditar es un proceso progresivo. La auditoría no cumple su objetivo si no hay seguimiento para determinar si la administración ha tomado las acciones correctivas apropiadas. Los auditores deben tener un programa para determinar si las acciones correctivas prometidas han sido tomadas bajo las recomendaciones de la auditoria.

El tiempo del seguimiento dependerá de lo crítico de los hallazgos y estarán sujetos al juicio y experiencia del auditor. Los resultados del seguimiento deben ser comunicados a los niveles de administración apropiados.

4.8. OTRAS TECNICAS DE EVALUACION Y AUDITORIA.

4.8.1. Analizar Documentación

* La corporación y el plan estratégico de procesamiento de información.

La corporación y el plan estratégico de proceso de información resume las metas de organización del centro de cómputo; las metas a largo y corto plazo, el presupuesto anual de operación, el plan de adquisición de hardware y la administración.

El mismo procedimiento de auditoría debe incluir el análisis del plan estratégico para determinar si las distintas clases de gastos departamentales han sido establecidos y seguidos, tales como hardware de computadora, mantenimiento de computadoras, adquisición de software, mantenimiento de software, etc.

* Diagramas de organización y funciones, resume la estructura de la organización e información, también muestra las responsabilidades de cada área funcional.

Los procedimientos de auditoria incluyen el diagrama de organización para conseguir una mejor comprensión de la responsabilidad que le corresponde a cada área funcional, y para determinar si cada centro de responsabilidad cuenta con el personal para satisfacer los requerimientos de servicio y recursos del usuario final, además, el auditor debe analizar la responsabilidad individual para asegurar la debida distribución de tareas.

* Políticas y procedimientos de operaciones

Las políticas y procedimientos de operaciones son establecidos para definir responsabilidades y proporcionar consistencia y eficencia dentro de las operaciones.

Los procedimientos de auditoria deben incluir un análisis de las políticas y procedimientos operacionales para asegurar que están establecidos adecuadamente por la administración y son cumplidos por los usuarios finales y personal que opera la computadora.

4.8.2. Observar al Personal Realizar sus Tareas

El procedimiento de auditoria debe incluir la observación del personal del centro de cómputo realizando sus tareas para determinar si los controles están en posición de asegurar la eficiencia y las operaciones, cumplimiento de las políticas y normas establecidas, supervisión adecuada y análisis de la administración del centro de cómputo la integridad y seguridad de los datos.

4.8.3. Tipos de Técnicas de Auditoria por Computadora.

Las técnicas computarizadas frecuentemente utilizadas son :

* Programas de recuperación y análisis.

Son programas de computación escritos de acuerdo con especificaciones de auditoría para organizar, combinar, calcular, analizar o extraer datos computarizados y para hacer cálculos y otras funciones de procesamiento computarizado como ayuda para nuestro trabajo de auditoría, específicamente para la obtención de evidencia sustantiva.

* Recuperación, análisis de datos y otras técnicas utilizando microcomputadoras.

- Downloading

Se puede transferir datos de un mainframe a microcomputadores (downloading) para revisarlos, estratificarlos, probar los cálculos, seleccionarlos, analizar estadísticas, etc. Estas técnicas permiten la transferencia de las pruebas de auditoría de un sistema de información central a un ambiente de trabajo individual.

- Técnicas de transacciones de prueba.

Estas técnicas prueban el software para obtener satisfacción de que los controles de procesamiento computarizado operan correctamente. Los controles de proceso y funciones de proceso computarizado son probadas mediante el ingreso (o intento de ingreso) de datos de prueba. Los resultados obtenidos del proceso son comparados con los resultados predeterminados.

Las técnicas de transacción de prueba son utilizadas para obtener evidencia de que los controles de proceso y funciones de proceso de cómputo operan en forma efectiva.

4.8.4. Técnicas Alternativas para la Obtención de Evidencia Sustantiva.

Una vez que se ha tomado la decisión de la técnica a utilizar para obtener evidencia sustantiva, se debe considerar la efectividad de las técnicas alternativas en relación a su costo.

Las consideraciones que el ASI debe hacer son :

* Software disponible,

* La disponisbilidad del personal del departamento de sistemas y la capacidad técnica del mismo,

* Los controles sobre los sistemas computarizados a evaluar,

* La experiencia y disponibilidad del ASI,

* La posibilidad de volver a utilizar los mismos programas en años futuros,

El ASI debe seleccionar los procedimientos más efectivos y eficientes en la auditoría. No obstante, las siguientes consideraciones ayudarán al ASI en el desarrollo de nuevas técnicas computarizadas a evaluar técnicas comunmente utilizadas.

* En primer lugar, es conveniente considerar que el personal que opera los sistemas desarrolle programas utilizando su propio software de recuperación.

* Considerar el uso de módulos de recuperación de datos del sistema.

* Considerar la relación costo/beneficio que el ASI adecue los programas utilizando el software de auditoría.

* "Enganches" (hooks) de auditoría

Los "hooks" de auditoría son puntos en los programas de aplicación denominados salidas (exits), que le permiten al ASI insertar comandos para procesos especiales de auditoría. Esta técnica permite al auditor modificar una aplicación estandar o un programa para llevar a cabo un proceso que respalde una actividad de auditoría.

Por ejemplo, un programa utilitario utilizado para reorganizar una base de datos puede incluír un "hook" para agregarle una codificación adicional que permita acumular totales de control y recortar registros de la base de datos.

Esto nos permite obtener totales de control en forma independiente y como subproducto del proceso normal del sistema

* Uploading

El uploading es el proceso inverso al downloading y consiste en la transferencia de datos desde un computador pequeño a uno más grande, por lo general un computador central. Un ejemplo de uso de microcomputador como herramienta de uploading es cuando el microcomputador se utiliza para crear programas de computación para luego ser transferidos y ejecutados en el computador central. Esto se ve habitualmente en el uso de paquetes "front end" para microcomputadoras, que se combinan con paquetes de recuperación o report writers de computadoras grandes

Otros ejemplos de uploading son:

* Uso del microcomputador como generador de datos de prueba con el fin de transferirlos al computador central. Los datos de prueba transferidos del microcomputador pueden ser procesados para propósito de auditoria.

* Los módulos de auditoria incorporados pueden ser programados en el microcomputador y transferidos para su difusión en el computador central. Si bien tales procedimientos normalmente son programados para su integración para los sistemas a auditar, este dispositivo proporciona al ASI flexibilidad y la posibilidad de ejecutar los programas al azar.

Los problemas técnicos del uploading son similares a los del downloading. Sin embargo, existen menos productos en el mercado con capacidad de uploading con conversión a los lenguajes del computador central. Por lo general, solo los paquetes más sofisticados de software (con aplicaciones integradas para computadores centrales y microcomputadores).

4.8.5. Software de Auditoria

Los paquetes de software de auditoría permiten la generación de programas de computación a través de especificaciones del usuario relativamente simples. Las instrucciones necesarias para realizar tareas típicas de auditoría no necesitan ser codificadas dado que la codificación está incluida en el paquete.

Para especificar las tareas de auditoría que deseamos que el programa ejecute, debemos proporcionarle información sobre el equipo de cómputo a ser utilizado y seleccionar la rutina o combinación de rutinas reprogramadas que deseamos.

Normalmente, la utilización de software de auditoría incluye cuatro etapas :

* Etapa 1 - Desarrollo de programa de auditoría específico.

Normalmente, los paquetes incluyen una biblioteca de rutinas de auditoría.

El programa generador construye un programa de auditoría basándose en los parámetros ingresados y en las rutinas de auditorías seleccionadas. El programa podrá ser utilizado de inmediato o guardado para su posterior utilización.

* Etapa 2 - Generación del programa fuente.

El programa codificado en la Etapa 1, es traducido a un lenguaje de alto nivel como, por ejemplo, COBOL. Como resultado, se obtiene un programa fuente que puede ser guardado para su posterior utilización o compilarlo de inmediato (vease Etapa 3). Por lo general, existe la posiblidad de aumentar la cantidad o complejidad de las tareas de auditoría agregando el programa fuente producido, el código escrito directamente en lenguaje de alto nivel. Las instrucciones adicionales del programa son normalmente denominadas "codificación propia".

* Etapa 3 - Compilación del programa fuente.

El programa fuente es procesado con el programa compilador, el cual lo traduce al lenguaje de máquina. El programa compilado se denomina programa objeto.

* Etapa 4 - Ejecución.

El programa objeto es ejecutado utilizando los datos a ser procesados y se generan informes.

Esta descripción general sobre el funcionamiento de software de auditoría es, obviamente, una simplificación.

Cada software de auditoría es único y diseñado para ser utilizado con determinado hardware y software. En la figura 4.1. se resume la forma en que operan dichos paquetes.

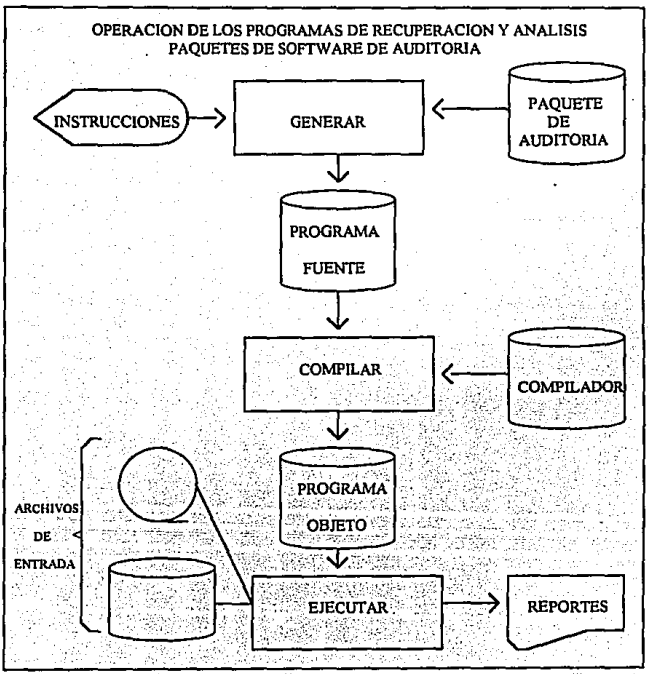


Figura 4.1.

El uso de software de auditoría tiene las siguientes ventajas.

* Han sido probados lo suficiente como para asegurar que funcionen en forma adecuada.
* Han sido diseñados para satisfacer las necesidades específicas de auditoría.
* Frecuentemente se disponen cursos de capacitación para su uso.
* Se puede obtener asistencia técnica para su utilización.

Sin embargo, existen ciertas desventajas comunes a todo el software de auditoría que debemos conocer, incluyendo limitaciones en :

* La cantidad de archivos que pueden ser leídos.
* La estructura de registros y representaciones de datos en archivos a los que se pueden acceder.
* La cantidad de selecciones y cálculos de auditoría que pueden especificarse.
* La posibilidad existente para formular expresiones lógicas y aritméticas en los archivos a evaluar.
* El número de informes de auditoría que pueden ser producidos en cada proceso de un archivo.
* El formato de los informes de salida.

4.8.6. Documentación de Auditoría en Informática.

La documentación es parte del ASI del control sobre las técnicas de auditoria en informática. La documentación de estas técnicas es similar a la de cualquier otra técnica de auditoría, con el fin de :

* Registrar las decisiones importantes, los procedimientos que se llevan a cabo, los controles existentes. y los resultados obtenidos.
* Facilitar la revisión del diseño y resultados de la aplicación.
* Documentar el trabajo realizado con los datos de salida.
* Facilitar el uso de la aplicación en años posteriores, proporcionando información de planificación que incluya detalles de problemas detectados y cambios recomendados.

4.8.7. Aspectos Sugeridos para Documentar la Auditoría en Informática.

Planificación

* Evidencia de auditoría específica a obtener.
* Descripción de la técnica computarizada seleccionada.
* Quién escribirá los programas de recuperación y análisis.
* Quién preparará los datos de prueba.
* Dónde y cómo serán procesados.
* Consideraciones sobre los controles.
* Personal necesario.

* Estimación del tiempo necesario.
* Estimaciones preliminares del costo/beneficio.
* Naturaleza del trabajo que se realizará con los datos resultantes.

4.8.8. Programa de Recuperación, Análisis y Documentación de Datos de Prueba.

* Descripción a detalle de los procedimientos de autidoría realizados (datos probados) mediante la aplicación de auditoría.
* Detalles de las rutinas probadas (edición, validación, cálculo, etc.).
* Detallar lo relativo a la preparación del programa, incluyendo en software y los controles usados durante el desarrollo.
* Especificaciones de la corrida, incluyendo entradas, pasos de procesos y salida de datos.
* Información de los sistemas, incluyendo diseño de archivos, formato de los registros, descripción de los campos y cursogramas.
* De qué forma fue probado el sistema.
* Documentación del programa final (listados de programas, flujogramas o descripción narrativa).
* Copias de las transacciones de prueba y resultados predeterminados.

4.8.9. Evidencia de Auditoría.

* Controles que afectan el proceso de la aplicación de auditoría.
* Los resultados obtenidos.

* Descripción a detalle del trabajo de auditoriia realizado sobre los resultados.
* Resolución de los errores, excepciones o partidas inusuales detectadas.
* Problemas administrativos y técnicos detectados y cómo fueron solucionados.
* Conclusión de auditoria.
* Recomendaciones a la Gerencia.
* Sugerencias de mejoras para años futuros.
* Comparación de costos reales con los presupuestados.

CAPITULO V
INTRODUCCION

Es una gran resposabilidad estar encargado de una área de auditoría informática en una organización, que podría contar con áreas de desarrollo, operación, telecomunicaciones y un computador grande y miles de archivos como apoyo a los usuarios. Obviamente no todas las instalaciones de procesamiento de datos son de este tamaño, de cualquier manera, en las instalaciones más pequeñas es normalmente imposible para el auditor, realizar una revisión detallada de todo el procesamiento de datos, así como la seguridad para que estos datos no sufran cualquier incidente. Por lo que nos hacemos la siguiente pregunta.

¿ Como puede realizarse la auditoria de tal manera que el ASI obtenga confianza de que la organización salvaguarda sus activos, mantiene la integridad de los datos y sus sistemas funcionan eficaz y eficientemente ?.

Por lo anterior, este capítulo provee un caso practico aplicando la metodología que describo en el capítulo cuatro, del camino utilizado para conducir una auditoría informática. Primero describe lo que es la planeación, después discute los pasos básicos para la elaboración de un programa de auditoría y finalmente examina algunas de la técnicas de obtención de evidencia, presentación y seguimiento del informe. Este proceso requiere que el ASI recopile evidencia, evalúe las fortalezas y debilidades de los controles basados en la evidencia reunida y prepare un informe de auditoría que presente los resultados de la misma de una manera objetiva para la administración, adheriendose a las normas y al uso adecuado de procedimientos y técnicas comunes en el desarrollo de auditorías. El ASI deberá entender los pasos y técnicas necesarias para planear, desempeñar y completar la auditoría.

5. APLICACION DE UN CASO PRACTICO

Antes de empesar con el caso practico, a continuación describo primero la forma como se compone un sistema contable, para así tener un mejor entendimiento del flujo de las operaciones computacionales de una empresa, de tal forma, que el estudio y la evaluación de un sistema se realizará de lo general a lo particular (estudiando primero el ciclo de operación para después evaluar el rubro en específico); ésto, dará al lector una mejor comprensión del sistema contable en su totalidad, ya que, se compone por ciclos operativos y éstos a su vez se componen en rubros.

5.1. CONCEPTO DEL FLUJO DE TRANSACCIONES

El estudio y evaluación de controles internos es el medio que utiliza el ASI para identificar y probar el riesgo de control. Por lo tanto, es una parte importante del planteamiento y las pruebas de auditoria. A la metodología utilizada para la comprensión de controles internos se denomina Concepto del Flujo de Transacciones. Los elementos fundamentales que soportan el concepto del flujo de transacciones son :

* Los tres componentes del sistema de control,
* El concepto de ciclos, y
* Los controles y procedimientos de sistemas de información computarizados.

5.1.1. Elementos del Sistema de Control

En general, la estructura de controles internos de una entidad consiste de tres componentes.

* El ambiente global de control gerencial
* El sistema contable
* Técnicas específicas de control

5.1.2. Ambiente Global de Control Gerencial

La gerencia crea el ambiente global de control y desarrolla las políticas y procedimientos para una supervisión continua y eficaz de las operaciones.

Los siguientes son ejemplos de controles gerenciales :

* Límites de autorización para adquisiciones de activo fijo
* Revisión de variaciones presupuestarias
* Auditoría interna
* Acceso restringido a información confidencial
* Política de aceptación del departamento usuario para la modificación de software del área de sistemas.

5.1.3. Filosofía y Estilo Operativo de la Gerencia

El impacto positivo o negativo del ambiente global de control gerencial sobre los informes financieros es consecuencia de los métodos o técnicas empleados por la gerencia y de su filosofía y estilo gerencial. La filosifía y estilo operativo de la gerencia comprende un amplio rango de características, como por ejemplo :

* Enfoque de la gerencia para aceptar y supervisar los riesgos del negocio;
* Actitudes y acciones de la gerencia hacia los informes financieros;
* Enfasis de la gerencia en el cumplimiento del presupuesto, resultados, y otros objetivos financieros y operativos.

El ambiente de control gerencial es menos eficaz cuando la gerencia acepta errores financieros, tolera el no cumplimiento con los procedimientos de control establecidos, o informes financieros para presentar mejores resultados. Por lo tanto, el ambiente global de control gerencial, tiene una influencia generalizada sobre el sistema contable.

5.1.4. Sistema Contable

El sistema contable incluye los métodos y registros establecidos para identificar, reunir, clasificar, analizar, registrar, e informar las transacciones de una entidad y la capacidad de definir responsabilidades específicas por los activos y pasivos relacionados.

Un sistema contable eficaz incluye procedimientos y documentos que :

* Identifican y registran todas las transacciones válidas.
* Describen oportunamente las clases de restricciones con suficiente detalle para permitir su clasificación en los informes financieros.
* Determinar el valor de las transacciones en una forma que permite registrar su valor monetario en los estados financieros.
* Determinar el periodo de tiempo en que ocurrieron las transacciones para registrarlas en el período contable adecuado.
* Presentan adecuadamente las transacciones y exposiciones relacionadas en los estados financieros.

5.1.5. Técnicas Específicas de Control

Las técnicas específicas de control son las técnicas detalladas de control que usa la gerencia para reducir el riesgo de error en los estados financieros. Los siguientes son ejemplos de técnicas específicas de control :

* Numeración correlativa y control
* Aprobación de las transacciones por personas autorizadas
* Uso de totales de control y conciliaciones de la entrada y salida de los sistemas de infirmación computarizados
* Referenciación cruzada de información de distintas fuentes

La combinación de técnicas específicas de control que se usan en un sistema contable reflejará la naturaleza y tamaño del negocio de la compañía, la naturaleza de su procesamiento de datos, y otros factores.

5.2. CICLOS Y FUNCIONES

Como se comentó anteriormente, las transacciones del sistema contable se segregan en ciclos de actividad del negocios (vease subprogamas capítulo II) para organizar el estudio y evaluación del plan de auditoría del ASI. El sistema contable de una compañía manufacturera comprenderá seis ciclos de transacciones.

* Tesorería,
* Egresos - Compras,
* Egresos - Nóminas,
* Conversión (transformación),
* Ingresos,
* Información financiera.

Cada ciclo se centra en los hechos económicos claves de las operaciones de la compañía.

5.2.1. Funciones de los Ciclos

Cada ciclo puede tener varios componentes (rubros o cuentas), los que se denominan "funciones". Una función es lo que se hace en el ciclo. Es un segmento de un sistema que procesa transacciones relacionadas lógicamente. La clase y cantidad de funciones de un ciclo varía en cada compañía.

Observemos mas detalladamente las funciones tipicas de cada uno de los seis ciclos. El ASI no debe esperar encontrar todos los ciclos ya que cada compañia se maneja segun sus actividades.

Ciclo deTesorería

El ciclo de tesorería incluye las funciones relacionadas con la administración de efectivo y la emisión de deudas de capital. Las funciones del ciclo de tesorería comienzan con el reconocimiento de las necesidades de efectivo. Incluyen la distribución del efectivo disponible a las operaciones y otros usos. Terminan con la devolución de los fondos a los inversionistas y prestamistas. El ciclo de tesorería puede incluir las siguientes funciones :

* Administración del efectivo e inversiones;
* Administración de la deuda;
* Venta de acciones ordinarias;
* Devengamiento y pago de intereses y dividendos;
* Custodia física del efectivo e inversiones, incluso la conciliación de saldos.

Ciclo de Egresos

El ciclo de egresos incluye los ciclos de: Egresos - Compras y Egresos - Nómina. En la mayoría de las empresas, las funciones relacionadas con la Nómina son totalmente diferentes de las relacionadas con las compras, y por lo tanto se clasifican en otro ciclo. Las funciones de estos ciclos son :

* Adquirir propiedades, bienes y servicios, y mano de obra, y
* Clasificar, resumir, e informar lo adquirido y lo pagado.

Las funciones del ciclo de egresos - compras incluyen :

* Selección de proveedores
* Pedidos
* Compras
* Recepción
* Control de calidad
* Cuentas a pagar
* Pagos

Las funciones del ciclo de egresos - nómina incluyen :

* Selección del personal
* Informes de asistencia
* Contabilidad de nómina
* Egresos de nómina

Ciclo de Conversión (Transformación).

Los recursos adquiridos por la entidad se mantienen, convierten, ensamblan, o usan de alguna otra forma durante el proceso de producción de sus bienes y servicios. Las funciones del ciclo de conversiones manejan recursos, tales como inventarios, y equipo y propiedades depreciables.

En el proceso productivo, los inventarios se "conviertен" en productos terminados mediante el uso de las plantas y equipos de la compañía. Luego, estos productos se venden a los clientes. Las funciones de este ciclo incluyen :

* Contabilidad de inventarios
* Inventarios físicos periódicos
* Contabilidad del activo fijo

Para un productor, el ciclo de conversión incluye las funciones claves para la generación de ingresos. Los otros ciclos y funciones existen para permitir esta conversión.

Las demás compañías tienen ciclos igualmente importantes, por ejemplo :

Industria	ciclo/actividad importante
Bancos	Préstamos
Comercio industrial	Ingresos
Construcción	Ingresos por contratos

Ciclo de Ingresos.

El ciclo de ingresos de una compañía incluye las funciones necesarias para intercambiar sus productos o servicios por dinero. Incluye :

* Entrada de pedidos.
* Despacho.
* Facturación.

* Cobranzas.
* Ajustes a las cuentas de los clientes.
* Administración a las cuentas de los clientes.
* Administración del crédito.

Ciclo de Información Financiera.

Este ciclo normalmente no procesa transacciones. En cambio, obtiene información contable y de otro tipo de los demás ciclos. Luego, analiza, evalúa, y resume esta información para que pueda ser enviada a la gerencia y a terceros. Sus funciones incluyen:

* Registro en el mayor general.
* Obtención de datos para información financiera adicional.
* Preparación de asientos de diario (si no se realiza en otros ciclos).
* Contabilidad de impuestos a las ganancias.
* Consolidación.
* Preparación de informes.

La tabla siguiente resume las actividades principales de cada cilclo y las cuentas más frecuentes :

CICLOS	ACTIVIDAD	EJEMPLOS DE CUENTAS DEL MAYOR GENERAL DEL CICLO
Tesorería	Administración de efectivo	Efectivo, Préstamos, Deuda a l/plazo,

		Patrimonio, Intereses
Egresos - Compras	Compra de vienes y servicios	Ctas. a pagar, varias cuentas de gastos de venta, generales y administrativos, como artículos de oficina, y Honorarios legales.
Egresos - Nóminas	Pago de sueldos y salarios	Mano de obra directa, Sueldos generales y administrativos.
Conversión (Transformación)	Proceso productivo de la compañía	Activo fijo, Depreciación acumulada, Inventarios.
Ingresos	Venta del producto o servicio de la compañía	Ventas, Comisiones de ventas, Cuentas a cobrar, Reserva para cuentas dudosas

Enlaces.

Si bien cada uno de los ciclos es independiente, existen interrelaciones entre los ciclos. Estas interrelaciones se denominan enlaces. Un enlace puede definirse como el punto donde una transacción sale de un ciclo y entra a otro. El asiento de diario para registrar cobranzas de los clientes es un ejemplo simple de un enlace.

El asiento de diario registra el hecho final del ciclo de ingresos (el pago del cliente por un producto o servicio de la compañía -- Débito : efectivo, Crédito : cuentas a cobrar). Una vez que se recibe el dinero, éste ingresa a la función de administración de efectivo, que está en el ciclo de tesoreria.

Esencialmente, los activos y las transacciones fluyen por los ciclos de la siguiente forma :

* El ciclo de tesorería brinda efectivo a los ciclos de egresos.
* Los dos ciclos de egresos compran materias primas y propiedades y pagan la nómina que se usa en el ciclo de conversión.
* El ciclo de conversión produce los bienes o servicios y controla el inventario hasta que los productos terminados están listos para ser vendidos.
* El ciclo de ingresos vende los productos o servicios. Pasa el dinero al ciclo de tesorería para su uso interno o su inversión externa.
* Todos los ciclos pasan la información contable de las transacciones que procesan al ciclo de información financiera. Allí, se la resume en los estados financieros.

La figura 5.1. muestra un diagrama que resume las interrelaciones entre los ciclos y el flujo de transacciones, efectivo, etc. :

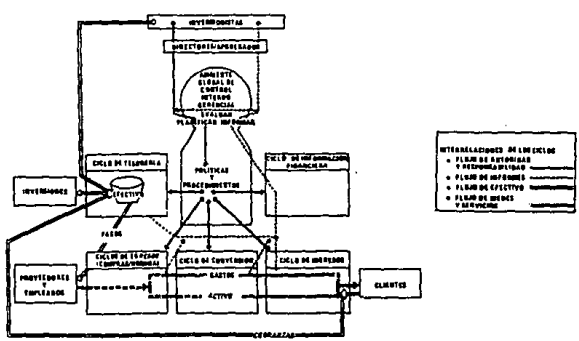


Figura 5.1.

A continuación muestro los ciclos que corresponden a los siguientes rubros de los estados financieros :

RUBROS DE LOS ESTADOS FINANCIEROS	CICLOS
Efectivo	Tesorería
Cuentas a Cobrar	Ingresos
Inventarios	Conversión
Activo fijo	Conversión
Depreciación acumulada	Conversión
Préstamos bancarios	Tesorería
Porción corriente de deuda a largo plazo	Tesorería
Cuentas a pagar	Egresos - Compras
Deuda a largo plazo,neta de la porción corriente	Tesorería
Ventas netas	Ingresos
Gastos de ventas, generales y administrativos	Egresos - Compras
Intereses pagados	Tesorería

Una vez que he descrito los ciclos de operaciones de una empresa, para la presentación del caso práctico, la auditoría de sistemas se enfocará al Ciclo de Ingresos para su rubro de Ventas y Cuentas por Cobrar.

5.3. CONOCIMIENTO DE LA EMPRESA

La siguiente descripción de las diferentes etapas de auditoría de sistemas tiene un enfoque desde el punto de vista auditoría externa, es importante la descripción de la empresa para tener un correcto entendimiento de las transacciones que genera.

5.3.1. Antecedentes de la Empresa

Estructura corporativa.

Ensambles Ultra S.A. de C.V. (EUSA), fue constituida en el estado de Nuevo León en la ciudad de Monterrey el 1 de abril de 1953, transformando una sociedad colectiva entre los señores Federico Espinosa y Manuel Torres en una sociedad anónima. La mayor parte del capital social es propiedad de los familiares de los fundadores y de la gerencia. Las acciones no cotizan en el mercado de valores, aunque la gerencia tiene planes para realizar una oferta pública.

Las oficinas generales de la Compañía y la planta manufacturera están ubicadas en la ciudad de México, D.F. La única instalación adicional es un almacén y oficina de ventas en Guadalajara, Jalisco.

Productos y características de la industria.

Ensambles Ultra S.A. de C.V. (EUSA) es una subsidiaria de un importante grupo empresario. Su actividad consiste en el diseño, armado, y manufactura de componentes diversos para sistemas hidráulicos, y accesorios.

Los productos de la Compañía conducen fluidos bajo condiciones variables de presión, movimiento, vibración y temperatura, utilizando mangueras flexibles o montajes metálicos tubulares (rígidos).

Las principales materias primas son acero, latón, tubos y mangueras (de goma y sintéticas). Cuatro industrias de manufactura (equipo para construcción, maquinarias, automotriz y camionera) conforman la mayor parte de su mercado. Un grupo diverso de otras industrias utilizan pequeñas cantidades de los productos de la Compañía. Los clientes pueden ordenar de una línea normal de productos o del catálogo de EUSA. La Compañía también realiza trabajos a pedido que deben ser diseñados individualmente para usos especiales. Todos los productos son manufacturados en la planta de Monterrey utilizando procesos macánicos y manuales. En términos generales, el costo de ventas está compuesto por aproximadamente 50 % de materiales, 15 % de mano de obra y 35 % de gastos de fabricación.

Los principales productos de EUSA son adaptadores, ensambles, empalmes y montajes para manguera. Los procesos de producción de estos productos son los normales para la industria de la manufactura de partes de equipo. Las barras de acero o de otro metal se taladran y cortan a un diámetro específico y según las especificaciones de empalmes. Los empalmes y adaptadores son luego moldeados hasta alcanzar las especificaciones de diámetro, empalme, plasticidad, etc.

El proceso de las mangueras comienza con el corte de las bobinas de manguera compradas hasta alcanzar su tamaño correcto. Luego, se corta nuevamente la manguera y se le prepara para unirla con las piezas de ensamble.

El proceso de producción para los montajes de tubo (más rígidos que los montajes de manguera) es muy similar al de los montajes de manguera, excepto por la maquinaria adicional que se requiere para doblar el tubo a sus ángulos exactos.

La Compañía tiene una fuerte competencia en todos los mercados que opera. Los competidores varian desde fabricantes muy pequeños de manguera y uniones hasta grandes grupos de empresas.

Son raros los cambios tecnológicos en la industria en que opera la Compañía y, por consiguiente, sólo se invierte anualmente una cantidad muy pequeña en investigación y desarrollo.

Mercado.

Los productos de la Compañía se ofrecen al mercado con una estructura de precios competitiva y tiene una reputación de alta calidad y servicio al cliente. Utilizando una estrategia agresiva de precios, la Compañía ha incrementado su participación en el mercado, pasando del octavo lugar en la industria con una participación de menos de 5 % al quinto lugar con una participación del 6 % del mercado. Este incremento se ha dado principalmente durante los últimos cinco años.

Alrededor del 55 % de las ventas de EUSA se hcen a distribuidores y comerciantes que operan principalmente en el mercado de consumidores finales (piezas de repuesto). El restante 45 % de las ventas se hacen a fabricantes de equipo original.

Las ventas de exportación son reducidas. Las ventas mensuales se realizan a aproximadamente 1,200 clientes.

El sistema de contabilidad.

En general, el sistema de contabilidad y de información financiera de la Compañía no tiene cambios con respecto al del año anterior. Consideramos que el sistema es adecuado para las necesidades de EUSA.

Los estados financieros mensuales y trimestrales se preparan a partir del mayor general generado por el área de sistemas. El mayor general es el resultado de un enlace entre los sistemas de ingresos, de inventario, de egresos y de nómina. Los resultados de la contabilidad de activos fijos preparados a través de una microcomputadora independiente son registrados en el mayor general por medio de asientos de diario mensuales. Además del enlace del sistema general con otros sistemas y de la contabilización de asientos de diario de activo fijo, el mayor general también se actualiza mediante otros asientos de diario recurrentes y no recurrentes. Los asientos de diario recurrentes son preparados por los empleados del departamento y aprobados por supervisores y por el contralor o el asistente del contralor. Los asientos de diario no recurrentes son preparados por el asistente del contralor y aprobados por el contralor.

Ciclo de ingresos.

La compañía procesa un promedio de 90 a 100 pedidos de venta por día. El importe promedio de un pedido es aproximadamente N$ 1,200.

El registro de ventas diarias, las facturas, el registro de pedidos pendientes (por falta de inventario para ser entregados en el futuro) y los informes de embarques son preparados en la computadora.

Los registros de inventarios y de cuentas a cobrar están integrados con el mayor general y el mayor general es conciliado con los registros detallados de inventarios perpetuos y con el auxiliar de cuentas a cobrar mensualmente.

Ciclo de egresos.

Las cuentas a pagar y otras erogaciones (gastos) afectan diariamente este ciclo generando salidas de efectivo, distribuciones de cuentas e informes de pagos. Se realiza un promedio de 500 pagos semanales. Se preparan cheques manuales para casos excepcionales, y cualquier importe en exceso de N$25,000 requiere de una segunda firma como un control de autorización. La Compañía procesa su nómina, incluyendo la distribución de la mano de obra directa al inventario, utilizando programas de computadora que están relacionados con los procesos productivos.

Ambiente de Sistemas.

Equipo ("Hardware")

La Compañía utiliza una computadora IBM AS/400 ubicada en su planta principal de Monterrey para la mayoría de sus procesos. Además, tiene una microcomputadora para la contabilización del activo fijo.

En los departamentos de contabilidad y en la planta existen terminales con capacidad para entrada de datos y consulta. Existe también una terminal localizada en el almacén de Guadalajara que se utiliza para ingresar pedidos, y que está conectada con la computadora central a través de un módem. No existe ningún otro proceso remoto. No han ocurrido cambios importantes este año en lo relacionado con el equipo de sistemas y no existen planes al respecto para el futuro cercano.

Aplicaciones y programas ("Software")

Programas de sistemas--Los programas son propiedad del proveedor y se utilizan mediante un convenio de arrendamiento. No se han hecho modificaciones a los sistemas, con excepción de aquellos recomendados por el proveedor como parte del mantenimiento, tal es el caso del sistema de ventas y cuentas por cobrar.

Sistemas de aplicación--Las aplicaciones incluyen el mayor general, el sistema de ingresos (que se utiliza para procesar pedidos de clientes, facturación, y cobranzas), el sistema de inventarios, el sistema de egresos (que se utiliza para las funciones de órdenes de compra a proveedores, cuentas por pagar y desembolsos), y el sistema de nómina.

Además, el activo fijo se controla por medio de una microcomputadora. Todas las aplicaciones fueron compradas a proveedores externos y modificadas por EUSA para cubrir sus necesidades específicas. No se ha hecho ninguna modificación importante a las aplicaciones este año y no existen planes al respecto para el futuro cercano.

Información.

El ingreso de información para el mayor general y para los sistemas de ingresos, egresos y nóminas se realiza en línea. La actualización de los archivos maestros se realiza mediante proceso por lotes todas las noches. El sistema de inventarios es un sistema de actualización tipo memorándum.

Personal.

Hay cinco empleados en el departamento de sistemas de EUSA: el gerente del departamento, quien reporta al tesorero, dos programadores y dos operadores. El gerente del departamento tiene diez años de experiencia en sistemas, mientras que los otros miembros tienen al menos dos años de experiencia en sus puestos.

A principios de 1990 la Casa Matriz del grupo comenzó a desarrollar un sistema computarizado de ventas y cuentas por cobrar el cual tiene interfase con el sistema de inventario. Luego de varias dilaciones, el sistema actual fué diseñado e implementado para su uso por la Casa Matriz en noviembre de 1991. Aproximadamente un año después, en enero de 1992, el sistema de ventas y cuentas por cobrar de EUSA fué convertido al que había implementado la Casa Matriz.

A principios de 1993 el sistema de ventas y cuentas por cobrar fue convertido de un antiguo sistema de IBM utilizado en las subsidiarias, a un sistema de mayor capacidad y más avanzada tecnología que se utiliza en la Casa Matriz en Monterrey.

Entre julio y septiembre de ese año se expandió el sistema, agregándole dispositivos interactivos de entrada de datos y de consulta directa a través de terminales on-line.

El sistema proporciona información de los clientes, registro de existencias y genera información gerencial.

Para cada registro de clientes y existencias contienen más de cincuenta datos distintos los cuales son continuamente actualizados. El personal autorizado puede acceder en forma directa a los registros, ya sea para actualizar o consulta. El sistema ha sido diseñado para procesar los requerimientos de pedidos, ventas, facturación, etc; así como recepción, despachos y para actualizar directamente todos los datos que sean necesarios para cualquier partida del sistema como proveedor, nivel de existencias para nuevos pedidos y precios unitarios.

Los niveles gerenciales apropiados reciben listados diarios de todas las transacciones procesadas por cada venta y sección. Además, y a efectos de llevar un registro histórico, se almacenan todas las transacciones que se realizaron desde que se implementó el sistema (aproximadamente 4,500,000). El personal operativo apropiado reciben diversos listados con información relativa a las partidas contenidas en el sistema.

Además se puede accesar por consulta directa al sistema a través de alguna de las 25 terminales instaladas, para obtener información relativa a las ventas realizadas y verificar el estado de cuenta de los clientes, así como información a cantidades disponibles, listados de recuento de existencias por unidad, listados de despacho ordenados por fecha prevista de entrega y último precio pagado para determinadas partidas de existencias.

5.4. ANALISIS DE RIESGO GENERAL 1994, IMPACTO DE FACTORES GENERALES DE ENSAMBLES ULTRA S.A. DE C.V.

5.4.1. Eventos del Año

Participación en el mercado/estrategia.

Continuando con la estrategia iniciada en 1992, la gerencia está utilizando un programa agresivo para elevar su participación en el mercado de poco menos del 5% a niveles por encima del 8%. El programa busca incrementar el uso de la capacidad instalada y requiere un crecimiento en las ventas por encima del promedio de la industria.

Para lograr este objetivo, los precios de venta han sido muy competitivos, produciendo una disminución en los porcentajes de utilidad bruta, pero aumentando el importe total de utilidad bruta.

En los primeros seis meses de 1994, las ventas han sido mayores que las alcanzadas en ese mismo periodo del año pasado, pero menores que las presupuestadas.

Mayores gastos de mercadeo y de entrega han reducido el resultado antes de impuestos por debajo de los niveles del año anterior. La gerencia espera alcanzar las ventas presupuestadas para 1994 gracias al fortalecimiento de la economía en general. Sin embargo, debido a la reducción de los márgenes y al incremento de los costos, el resultado antes de impuestos será menor que el presupuestado.

Cuentas a cobrar.

Durante los primeros 6 meses de 1994 el saldo de las cuentas a cobrar ha aumentado en $300,000, 9% por encima del saldo al 31 de diciembre de 1993. Si bien se esperaba un incremento estacional, se ha producido también un incremento en los días de venta en cuentas a cobrar. El incremento de la participación de la Compañía en el mercado ha traido como consecuencia nuevos clientes y el incremento de los saldos a cobrar a los antiguos clientes. El gerente de crédito está al tanto de este problema y ha implantado medidas tendientes a reducir la antigüedad de las cuentas a cobrar.

Personal de contabilidad.

Los problemas de rotación en el área de contabilidad han continuado durante 1994. Este problema se deriva de las agresivas políticas de reclutamiento en el mercado local para con los empleados administrativos. Sin embargo, los recientes incrementos en los beneficios de la compañía han sido positivos para el reclutamiento y retención de empleados.

Gracias a la directa participación del personal responsable del departamento de contabilidad, se ha logrado cumplir con las responsabilidades diarias del área. Sin embargo, se nos ha solicitdo nuestra opinón sobre deficiencias en el desempeño y entrenamiento del nuevo personal.

Análisis financiero.

Conjuntamente con los programas de mercadotecnia y los objetivos de crecimiento en las ventas antes mencionadas, existe cierta presión por parte de la gerencia para alcanzar los resultados presupuestados. Si bien las operaciones del año se encuentran por debajo de lo normal desde un punto de vista histórico, la posición financiera es sólida. La gerencia espera alcanzar el resultado antes de impuestos presupuestados durante el segundo semestre del año. Tendremos en cuenta el riesgo que estas presiones sobre las ventas y los resultdos representan. La posición financiera de la compañía es sólida y su índice corriente es adecuado.

Condiciones de la industria.

El ramo está experimentando los efectos de los incrementos en las ventas de las industrias automotriz y de la construcción. Las utilidades netas están reaccionando favorablemente a las bajas tasas de interés sobre deudas a corto plazo y a la disminución de los índices inflacionarios en las materias primas.

Se espera que continúe el incremento en compras o bienes de capital durante 1995. EUSA y sus competidores están también observando fuertes incrementos en las ventas a los mercados de partes de repuesto.

Ambiente de controles gerenciales.

La revisión de controles gerenciales que acabamos de concluir, indican que continúa fomentando una actitud favorable hacia los controles. A pesar de que la mayoría de los procedimientos no se encuentran formalmente documentados, los procedimientos financieros y de presupuestación se encuentran claramente definidos y continúan siendo fuertes.

Ambiente de sistemas.

El ambiente de sistemas de EUSA fue clasificado como "B"-bajo por el programa EDP-RISC, clasificación con la cual el equipo de auditoría está de acuerdo. EUSA cuenta generalmente con aplicaciones sencillas de sistemas utilizadas en la mayoría de los

procesamientos de transacciones y de información financiera. Nuestra revisión de los controles generales EDP fue hecha por el encargado de la asignación, quien cuenta con experiencia en auditoría de sistemas . Los resultados de nuestra revisión de los controles generales han sido documentados en un memorándum. El siguiente párrafo resume los resultados de dicha revisión y su impacto general en el enfoque de la auditoría.

Existe riesgo debido a la falta de segregación de funciones asi como por el limitado número de personal y su acceso a los programas, la información existente y a la documentación de la computadora. Debido a que ninguna de las aplicaciones de EUSA es compleja, esas debilidades no deberán tener un impacto importante en nuestro plan de auditoría.

En la medida en que confiemos en información generada por los sistemas, ejecutaremos pruebas sobre los controles de entrada/salida de los departamentos usuarios o pruebas substantivas sobre la información misma.

5.4.2. Resumen de Riesgos de Auditoría

Riesgos de error en los estados financieros.

El riesgo potencial de errores significativos en los estados financieros se considera bajo, por las siguientes razones:

La Compañía ha gozado de una posición financiera relativamente fuerte. Si bien, ha experimentado una reducción de sus ingresos durante los primeros seis meses, ha mantenido una posición financiera sólida y el capital de trabajo no se ha visto afectado negativamente.

No existen rubros que sean resultado de transacciones, cálculos o estimaciones complejos.

En los últimos año no ha habido problemas contables o de exposición importantes. La Compañía no tiene políticas contables inusuales o controversiales. No se han propuesto ajustes significativos en el pasado, excepto por diferencias de juicio en las áreas de cobrabilidad de clientes, reservas por exceso y obsolescencia de inventarios, e impuestos federales, donde nosotros determinamos los asientos de fin de año.

El ambiente general de controles gerenciales es adecuado y la gerencia mantiene una actitud positiva hacia los controles. Las políticas y procedimientos se encuentran bien definidos. La gerencia es receptiva y accesible respecto de las recomendaciones sobre control interno.

La gerencia y el Comité de Auditoría Interna revisan mensualemente los estados financieros e investigan cualquier fluctuación o variación presupustaria inusual. Se entregan estados financieros trimestrales a todos los accionistas, acreedores, para su revisión y comentarios.

Riesgos de irregularidades.

El riesgo de irregularidades importantes se considera bajo, debido a las siguientes razones:

El grupo propietario y los miembros claves de la gerencia han estado con EUSA por varios años y no hay historia de irregularidades. Además del efectivo, no hay otro activo que sea fácil o rápidamente convertible. El grupo propietario es fácilmente accesible y la gerencia ha sido receptiva de nuestras recomendaciones en años pasados.

Existe, por parte del grupo propietario, un fuerte y activo control de las actividades financieras, de inversión y sobre el presupuesto de capital. Los gastos capitalizables superiores a N$25,000 requieren la participación directa de dos miembros autorizados de la gerencia, a través de la firma de los cheques. Las cobranzas se manejan mediante una cuenta de apartado de correos.

Trimestralmente, se revisan los estados financieros mensuales y otros informes, investigándose partidas anormales, variaciones, etc. Asimismo, se entregan trimestralmente estados financieros a los acreedores de la Compañía, para su revisión y comentarios.

El riesgo de sistemas se considera bajo. Los riesgos existentes pueden cubrirse con pruebas de cumplimiento y substantivas.

Problemas potenciales del negocio en marcha.

No existen dudas sobre la viabilidad de la Compañía como negocio en marcha debido a su posición establecida en el mercado, su relativa sólida posición financiera, su importante patrimonio, y sus operaciones históricamente rentables. Los márgenes brutos son menores que en el pasado. Sin embargo, la Compañía está enfrentando esta situación y se esperan requerimientos normales de capital de trabajo y de otros flujos recurrentes de efectivo. Continuaremos vigilando esta situación, pero no creemos que exista un problema que requiera un mayor trabajo de auditoría. Revisaremos los resultados finales en busca de posibles indicios de deterioro de la situación.

Enfoque y alcance general de la auditoría.

Con base a nuestra evaluación de los factores significativos descritos, nuestra evaluación del ambiente general de control y nuestra experiencia anterior, el enfoque general de auditoría depositará una confianza significativa en los controles generales, especialmente en los controles gerenciales, y enfatizará lo siguiente :

- Uso selectivo de procedimientos de revisión analítica y predictivos, dada la eficacia de los controles gerenciales y la naturaleza del negocio.
- Alcances moderados en nuestras pruebas substantivas y en nuestras pruebas de controles. Reduciremos algunos alcances respecto del año anterior, con excepción de nuestro trabajo de cortes y de análisis de ventas, donde ampliaremos nuestros alcances debido a que se espera un incremento de ventas en lo que resta del año.

-Se utilizarán pruebas especificas sobre algunas transacciones que requieren estimaciones basadas en información no financiera.

Existe un riesgo potencial mínimo de exposiciones o clasificaciones incorrectas en los estados financieros, debido a que la Compañía no realiza transacciones complejas ni requiere de exposiciones complicadas de información

Nuestra confianza en los controles significativos está soportada por nuestro estrecho contacto con el cliente durante el año mediante reuniones trimestrales. La Compañía nos consulta cualquier transacción inusual o significativa que pueda tener un efecto significativo en los estados financieros.

Prepararemos un análisis de riesgo de cuentas en donde resumiremos las relaciones esperadas entre cuentas, las cuales relacionaremos con el ambiente de control interno y realizaremos un esbozo preliminar del tipo de trabajo de auditoría a completar.

Considerando la presión de la gerencia por lograr los objetivos presupuestados, incrementaremos nuestro alcance en las pruebas de corte a fin de año, y en las de ventas.

Coordinación y oportunidad.

El trabajo de planeamiento y la revisión de información trimestral al 30 de junio se ejecutó durante la primera semana de agosto de 1994. La observación de inventarios físicos y el trabajo de circularización sobre cuentas a cobrar se hará al 31 de octubre de 1994, probándose posteriormente el movimiento de las cuentas hasta el cierre del ejercicio. Nuestro trabajo de prueba de controles se ejecutará durante las primeras dos semanas de la visita de noviembre y nuestro trabajo final se hará durante las últimas dos semanas de enero de 1995.

La presentación de la declaración de impuesto a las ganancias será diferida. El 1o. de agosto de 1994 se llevó a cabo una reunión de planeamiento del equipo de auditoría interna, en la cual se discutió el enfoque general de auditoria.

5.5. RESUMEN DE RIESGOS GENERALES DE SISTEMAS Y EVALUACION DE CONTROLES

Como parte de nuestro trabajo de planeamiento de la auditoría y evaluación del riesgo, hemos evaluado la naturaleza de los riesgos y controles de sistemas de EUSA. El propósito es documentar nuestra evaluación mediante:

-La documentación de la naturaleza y principales características del ambiente de sistemas.

-La documentación de la importancia y complejidad de sistemas para la información financiera y las operaciones de EUSA, y

-Un resumen del alcance, resultados e impacto en el plan de auditoría de nuestra evaluación de los controles de sistemas.

Antecedentes de Sistemas

Información general

El gerente del departamento de sistemas, es responsable del manejo de los sistemas de información de EUSA. A la fecha, el departamento de sistemas tiene cinco personas.

La mayoría del procesamiento de datos de EUSA se realiza en Monterrey usando su computadora IBM AS/400. Todo el procesamiento se hace en las oficinas centrales, pero la división de ventas de Guadalajara ingresa algunas órdenes.

5.5.1. Eficiencia del Control Gerencial

Encontramos que EUSA ha asignado responsabilidades para la función de sistemas y ha establecido una abierta comunicación entre el área de sistemas y los usuarios. Esto genera un ambiente positivo para unos sólidos controles generales y de aplicación de sistemas, y minimiza la frecuencia y gravedad de problemas relacionados con sistemas que pudiesen generar errores en los estados financieros.

5.5.2. Riesgo y Complejidad del Área de Sistemas

Utilizando el "software"de los auditores en sistemas "EDP-RISC" (Sistema para clasificar el riesgo y complejidad del sistema), hemos clasificado a EUSA como "B"-bajo. Para llegar a dicha clasificación, consideramos factores tales como el nivel de confianza en los controles de sistemas previsto, la complejidad de los sistemas de EUSA y las expectativas de la Compañía en el área de sistemas.

El sistema de contabilidad.

EUSA utiliza su computadora para procesar órdenes recibidas, despachos, facturación, y otras funciones vitales de la Compañía. Consideramos que los siguientes sistemas son importantes para los informes financieros y las operaciones de EUSA:

-Sistema de ingresos - Ordenes recibidas, cuentas a cobrar y cobranzas.
-Sistema de egresos - Cuentas a pagar y desembolsos
-Mayor general - Preparación de estados financieros

Determinamos que estos tres sistemas son simples ya que los volúmenes de transacciones son moderados, la lógica del proceso parece sencilla, y generalmente las pistas de auditoría son completas. Estimamos que existen adecuados controles del usuario, los que permiten el logro de la mayoría de los objetivos de control.

Nuestro plan de auditoría confía en los controles de las aplicaciones de cuentas a cobrar, ya que las confirmamos a fecha preliminar.

En consecuencia, nuestra revisión del departamento de sistemas se concentró en identificar las debilidades importantes en los controles generales de sistemas que pudiesen afectar el sistema de cuentas a cobrar. A continuación se muestra en la figura 5.2. un esquema del flujo de transacciones en la función de cuentas por cobrar.

FUNCION DE CUENTAS A COBRAR

PROCESAMIENTO AL FINAL DEL MES

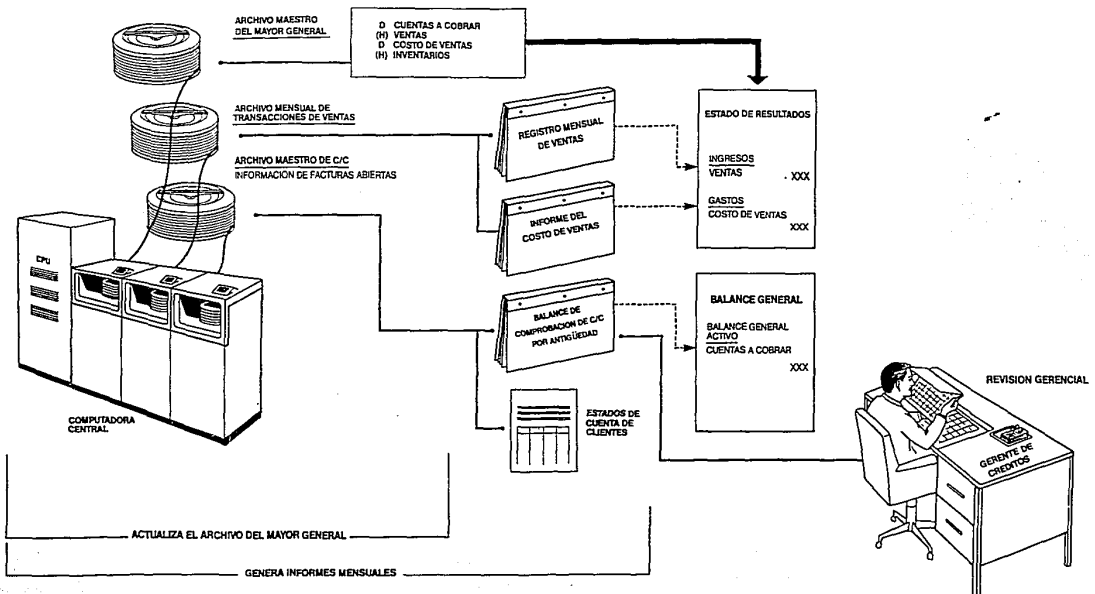


Figura 5.2.

Alcance, revisión de los controles de sistemas.

El gerente de sistemas realizó la revisión de EUSA en julio de 1994. La revisión consistió principalmente en lo siguiente:

- Entrevistamos al gerente de sistemas y al gerente de operaciones para comprender los distintos controles y procedimientos relacionados con el ambiente de controles generales de sistemas.
- Donde lo consideramos adecuado, revisamos documentación para respaldar las afirmaciones de la Compañía, por ejemplo: formas de solicitud del usuario, programas de uso diario de equipo, formas de autorización, etc.
- Recorrimos el sector de operaciones donde se localiza el equipo para evaluar la seguridad física y la organización en esta área.
- Probamos los parámetros críticos de control y las secciones de los principales "software" de sistemas que brindan seguridad lógica a los procesos por lote y en línea dentro del ambiente de la IBM AS/400.
- Probamos mecanismos lógicos de control específicos que impiden el acceso no autorizado a programas y archivos (por ejemplo,sistemas de seguridad para control de accesos en línea y sistemas de seguridad para procesamiento por lotes).
- Con base a entrevistas, observaciones y otras pruebas de los controles, determinamos las técnicas de control en el área de sistemas.

- Una vez completada, evaluamos toda la información recolectada, determinando si se cumplen los objetivos de control.

5.6. EVALUACION DEL AMBIENTE DE CONTROLES GENERALES DE SISTEMAS COMPUTARIZADOS

Los controles generales comprenden los controles que forman el ambiente en el que operan las aplicaciones de sistemas. Debido a su naturaleza, unos controles generales débiles podrían impactar negativamente cada aplicación de sistemas. Los controles de los usuarios pueden brindar una suficiente cantidad de controles sobre las aplicaciones; sin embargo, un buen ambiente de controles generales de sistemas disminuye el nivel de confianza necesario en los controles de usuarios.

En nuestra revisión, observamos que las técnicas generales de control de sistemas no fueron suficientes para cubrir los riesgos potenciales de todas las áreas de control de sistemas. Específicamente, observamos debilidades en las siguientes áreas de control de sistemas:

- **Segregación de funciones**: Debido al tamaño del departamento de sistemas, no existe una segregación adecuada de tareas entre las funciones de sistemas.

- **Control sobre el acceso a la información**: El personal de sistemas puede hacer modificaciones no autorizadas a la información mediante el uso de ciertos utilitarios que pueden evitar los mecanismos de seguridad lógica existentes.

5.6.1. Impacto en la Auditoría

Dado el ambiente de controles generales descrito con anterioridad, incluiremos los siguientes pasos en nuestro plan de auditoría.

- Debemos identificar y probar los controles de los usuarios sobre entradas, salidas y procesamiento de las transacciones. Enfatizaremos en nuestra revisión los controles relativos a procesos de compatibilidad (por ejemplo: segregación de funciones, regularidad, formalidad, revisión y aprobación por un supervisor, documentación adecuada, disposición de partidas de conciliación, etc.).
- Debemos probar la corrección aritmética de los informes generados por la computadora en los cuales confiaremos. Además, debemos hacer referencia cruzada a nuestros papeles de trabajo donde se realiza el trabajo sustantivo.

Estas pruebas incluirán como mínimo:

a) Verificación de sumas, particularmente las relacionadas con balances de comprobación.
b) Verificación de la corrección de algoritmos claves que no son probados por la Compañía (por ejemplo: antigüedad de cuentas a cobrar, valuación de existencias de inventarios, etc.).

Debemos cotejar nuestras pruebas detalladas sobre transacciones específicas con los informes generados por las aplicaciones para asegurar que están incluídas completa y correctamente en el mayor general y en los estados financieros.

Debemos entrevistar al personal de supervisión de todos los departamentos usuarios de los sistemas de aplicación que afectan significativamente la información financiera. En este proceso de entrevistas, debemos determinar el grado de satisfacción de los usuarios y si hubo problemas importantes durante el año pasado que hubiesen sido originados por la calidad de los programas de aplicación.

5.7. FACTORES DE RIESGO INHERENTE Y DE CONTROL PARA EL SISTEMA DE VENTAS Y CUENTAS POR COBRAR.

Durante la planificación detallada debemos estar alertas a los factores o condiciones que puedan afectar nuestra evaluación del riesgo inherente y de control. Antes de seleccionar los procedimientos de auditoría debemos considerar el impacto de los factores de riesgo observados durante la planificación estratégica y aseguramos de que nuestro plan de auditoría toma en cuenta adecuadamente dichos riesgos.

Aunque nuestra atención está normalmente concentrada en las áreas de mayor riesgo, siempre debemos estar alertas a la posiblidad de reducir nuestro alcance de auditoría en las áreas de menor riesgo.

5.7.1. Factores de Riesgo Inherente

Un anáisis de la información sobre el componente para los distintos períodos puede identificar situaciones de riesgo. Las transacciones nuevas o significativas a menudo representan áreas de mayor riesgo.

* Existe una cantidad significativa de nuevos deudores.
* Los procedimientos de cobranza han sido significativamente modificados.
* Los productoss destinados a la venta están sujetos a cambios significativos de precios.
* El cliente depende de un reducido número de deudores o de contratos de precio fijo.
* La introducción de nuevos productos de los competidores ha alterado la participación de mercado y los márgenes brutos.
* Se utiliza un método complejo de estimación de los ingresos por ventas (por ejemplo, el método de porcentaje por grado de avance)
* Las ventas son contabilizadas aún cuando existe el derecho de devolución.
*Las ventas son reconocidas cuando las cuentas a cobrar relacionadas han sido descontadas con derecho a reclamo

posterior en caso de incobrabilidad.

* Existen compromisos de ventas adversos.
* Aumentan las devoluciones de productos vendidos.
* Las estimaciones de la gerencia de los niveles de devoluciones, descuentos, bonificaciones y deudores incobrables no fueron correctas.
* Existe un deterioro significativo en la antigüedad de las cuentas a cobrar.
* Los deudores pertenece a industrias que están experimentando condiciones desfavorales.
* Existen transacciones significativas entre empresas vinculadas.

5.7.2. Factores de Riesgo de Control

* No se han preparado análisis confiables de cuentas vencidas.
* Ha habido un aumento significativo en la cantidad y monto de notas de crédito o ajustes.

* Los límites de crédito son informales y no están sujetos a autorizaciones.
* Las cantidades despachadas frecuentemente difieren de las cantidades pedidas.
* Han aumentado las notas de crédito o devoluciones, ajuste de precios o errores de cálculo.
* Han aumentado las quejas de los deudores con respecto a sus cuentas.
* Los créditos otorgados pueden ser procesados sin autorización.
* Existen desvíos en los procedimientos de cobranzas.
* Existe una acumulación de transacciones no procesadas.
* Existen numerosas partidas pendientes en las conciliaciones de los registros auxiliares con las cuentas de control del mayor general.

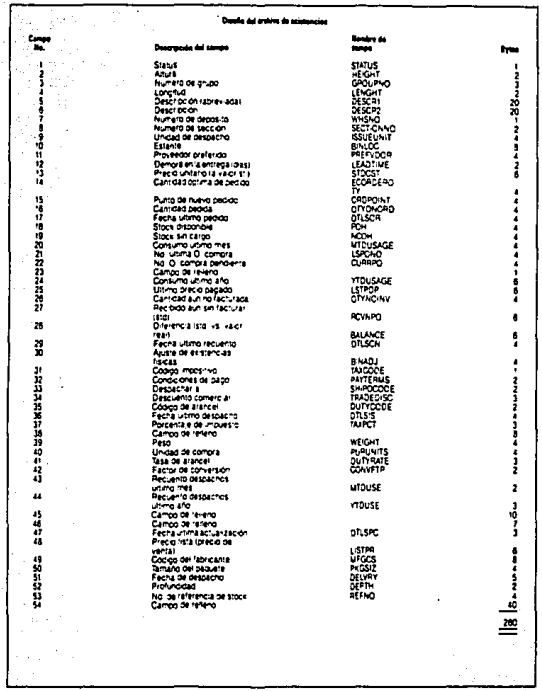
5.8. ANTECEDENTES DE AUDITORIA

Anteriormente los procedimientos de auditoría utilizados para probar exactitud, integridad y corrección se llevaban a cabo mediante indagación, observación, recálculo y a través de referencias de documentos fuente. No se había considerado seriamente el desarrollo de programas de recuperación y análisis ya que se sabía que el sistema de cuentas por cobrar y existencias iba a ser transformado, adoptando el diseño que implementaron en la Casa Matriz. La conversión del sistema ya ha sido completada. Los requerimientos de auditoría fueron presentados por el auditor en sistemas responsable del grupo que realizará la revisión por medio de la siguiente carta dirigida al gerente del área de sistemas.

Ref.: **Programa de Recuperación y Análisis para Ventas, Cuentas por Cobrar y Existencias**

El propósito de esta carta es documentar, para referencia futura, el estudio de factibilidad llevado a cabo la semana pasada conjuntamente con nuestro especialista de auditoría en sistemas. Visitamos las oficinas de EUSA para evaluar la posiblidad de utilizar su software de auditoría a fin de llevar a cabo gran parte de la revisión prevista en el plan de auditoría para el rubro de cuentas por cobrar y existencias.

Identificamos el archivo a utilizar, del cual le adjunto una copia del diseño de sus campos con las explicaciones necesarias como se muestra en la tabla 5.3.



Diseño del archivo de existencias

Campo No.	Descripción del campo	Nombre de campo	Bytes
1	Status	STATUS	1
2	Altura	HEIGHT	2
3	Número de grupo	GROUPNO	3
4	Longitud	LENGHT	3
5	Descripción abreviada	DESCR1	20
6	Descripción	DESCR2	20
7	Número de depósito	WHSNO	1
8	Número de sección	SECT-CANO	2
9	Unidad de despacho	ISSUEUNIT	4
10	Estante	BINLOC	3
11	Proveedor preferido	PREFVDOR	4
12	Demora en la entrega (días)	LEADTIME	2
13	Precio unitario de reposición	STDCST	6
14	Cantidad óptima de pedido	ECORDERQTY	4
15	Punto de nuevo pedido	ORDPOINT	4
16	Cantidad pedida	QTYONORD	4
17	Fecha última pedida	DTLSOR	4
18	Stock disponible	POH	4
19	Stock sin cargo	NOOH	4
20	Consumo último mes	MTDUSAGE	4
21	No. última O. compra	LSPONO	4
22	No. O. compra pendiente	CURRPO	4
23	Campo de relleno		1
24	Consumo último año	YTDUSAGE	6
25	Último precio pagado	LSTPOP	6
26	Cantidad aún no facturada	QTYAGINV	4
27	Recibido aún sin facturar (stock)	RCVNPO	6
28	Diferencia lista vs. valor real	BALANCE	6
29	Fecha último recuento	DTLSCN	4
30	Ajuste de existencias físicas	BINADJ	4
31	Código impositivo	TAXCODE	1
32	Condiciones de pago	PAYTERMS	2
33	Despachar a	SHPCODE	3
34	Descuento comercial	TRADEDISC	3
35	Código de arancel	DUTYCODE	2
36	Fecha último despacho	DTLSIS	4
37	Porcentaje de impuesto	TAXPCT	3
38	Campo de relleno		8
39	Peso	WEIGHT	4
40	Unidad de compra	PURUNITS	4
41	Tasa de arancel	DUTYRATE	3
42	Factor de conversión	CONVFTP	2
43	Recuento despachos último mes	MTDUSE	2
44	Recuento despachos último año	YTDUSE	3
45	Campo de relleno		10
46	Campo de relleno		7
47	Fecha última actualización	DTLSPC	3
48	Precio lista (precio de venta)	LSTPR	6
49	Código del fabricante	MFGCS	8
50	Tamaño del paquete	PKGSIZE	4
51	Fecha de despacho	DELVRY	3
52	Profundidad	DEPTH	4
53	No. de referencia de stock	REFNO	4
54	Campo de relleno		40
			260

Figura 5.3.

Se puede acceder con facilidad a este archivo empleando el software de auditoría de la compañía. En el pasado no hemos tenido problemas de disponibilidad de tiempo del computador. El archivo de cuentas por cobrar y existencias es preparado semanalmente, pero como los informes más importantes son preparados en forma mensual creo que será más conveniente usar la copia de un fin de mes. Si bien el momorándum de planificación establece que todo el trabajo se llevará a cabo sobre saldos al 30 de septiembre, creemos conveniente volver a ejecutar el programa al cierre del ejercicio para obtener evidencia de auditoría adicional. Propongo los siguientes requerimientos detallados para este programa:

* Revisaremos las sumas y multiplicaciones del archivo, obteniendo subtotales por sección.
* Sumar las partidas recibidas y aún no facturadas a fin de verificar que la provisión sea adecuada.
* Comparar el costo estándar con el último precio pagado y listar las partidas en las que la diferencia sea muy significativa.
* Listar las partidas de poco movimiento, comparando el uso durante el año con la cantidad de existencias.
* Listar las existencias significativas que no hayan sido recontadas durante alguno de los recuentos físicos cíclicos que realizó EUSA durante el año.
* Listar los ajustes de existencias más significativos.
* Seleccionar una muestra de materiales para hacer un control detallado de costos.
* Listar las partaidas en las cuales el stock disponible esté muy por debajo del punto de nuevo pedido.
* Listar las partidas recibidas aún no facturadas con un saldo significativo.

* Listar todas las partidas con stock negativo.
* Listar las existencias con valor cero.
* Listar las partidas en las cuales la unidad de compra sea distinta a la unidad de despacho.

El análisis preliminar de costo/beneficio realizado para el programa de recuperación y análisis de cuentas por cobrar y existencias debería ser modificado a 118 horas (de las cuales ya hemos ocupado 16) para tareas de desarrollo y 78 horas de ahorros identificados por la reducción de procedimientos manuales. Basándome en la mayor satisfacción de auditoría que creo se obtendrá al poder aplicar nuestras pruebas a todo el archivo, sugiero se proceda a utilizar los procedimientos de auditoría de sistemas por el computador. Agradeceré me haga saber:

* Si está o no de acuerdo con el procedimiento.
* Cuáles de las pruebas mencionadas desea realizar sobre los saldos al 30 de septiembre y cuáles desea repetir al cierre del ejercicio.
* Si tiene alguna preferencia en cuanto a límites de valor para cada prueba o si tiene alguna sugerencia relativa a pruebas adicionales que se podrían incluir en el programa.

5.9. DESARROLLO DEL PROGRAMA DE AUDITORIA

Un programa de auditoría es un grupo de procedimientos documentados, diseñados para llevar a cabo los objetivos de auditoría planeados.

Es importante destacar que los sistemas contables funcionan de manera similar, pero en ocasiones difieren en procedimientos, por lo cual, el ASI deberá tener la suficiente capacidad para desarrollar programas de auditoría a la medida del sistema a auditar, adaptándolo a las circunstancias.

5.9.1. Consideraciones sobre el Negocio

Al desarrollar un programa de auditoría, el ASI deberá contemplar algunos aspectos importantes de la organización y para el sistema en específico a auditar; en este caso, para el sistema de ventas y cuentas por cobrar son :

Líneas de productos, métodos de comercialización y políticas de distribución.

* Los tipos de productos vendidos y los montos correspondientes.
* Cambios significativos en las ventas.
* La naturaleza de cualquier cambio en las líneas de productos o de servicios.
* Si se otorgan descuentos o bonificaciones especiales cuando se introduce un nuevo producto.
* La naturaleza estacional del negocio, entre otros.

Características de los deudores.

Las características de los deudores pueden afectar nuestro enfoque de auditoría en áreas tales como la evaluación de riesgos, parte sustancial el cobrar y previsiones para volumen de ventas.

Condiciones y tendencias económicas de los mercados.

Cuando una economía crece, puede aumentar la rentabilidad pero se requerirá un mayor capital en el trabajo. En una situación económica adversa, las cobranzas son más lentas y la disminución de las ventas puede afectar las posibilidades del cliente de mantener su negocio.

Aplicación de procedimientos de diagnóstico.

Los procedimientos de diagnóstico proporcionan evidencia de auditoría útil y, cuando son ampliados para cubrir todo el período pueden representar una parte importante de la evidencia de auditoría requerida.

Consideraciones de cuestiones contables significativas.

Debemos considerar cuidadosamente el impacto que los cambios en los principios contables u otros temas contables pueden causar en, nuestra evaluación del riesgo y en el enfoque de auditoría.

Actualización de sistemas.

Una actualización de sistemas involucra una revisión de los sistemas a evaluar con el fin de actualizar los conocimientos acumulados de los sistemas contables y de control en el área de ventas y cuentas por cobrar para :

* Evaluar si los riesgos inherentes previamente identificados han sido considerados por los controles del sistema, por ejempo, debemos confirmar las evaluaciones previas de los riesgos de control;
* Confirmar si los controles o las funciones de procesamiento computarizados constituyen una base confiable; o
* Facilitar la programación de procedimientos sustantivos.

Una actualización de sistemas puede realizarse siguiendo el rastro de una pequeña cantidad de transacciones (posiblemente una o dos de cada tipo) a través del sistema. Las pautas proporcionadas para la ejecución de una actualización de sistemas están dirigidas a los aspectos importantes del flujo de transacciones a través del sistema de ventas y cuentas por cobrar, concentrándose en las características de los sistemas que son de interés para el ASI. El propósito de una actualización de sistemas es confirmar estos conocimientos e identificar los cambios relacionados con los aspectos importantes del flujo de transacciones a través del sistema que pudieran afectar nuestro enfoque de auditoría, y puede incluir una evaluación de los controles directos (es decir, controles gerenciales e independientes, controles de procesamiento y funciones de procesamiento computarizados y controles para salvaguarda de activos) y, si se espera confiar en dichos controles directos, de los principales controles generales.

Una actualización de sistemas también ayuda a confirmar si el sistema contable continúa proporcionando una base adecuada para la preparación de los estados financieros. Si la actualización de sistemas se realiza con este objetivo, se deberá otorgar mayor énfasis a los aspectos de procesamiento del sistema a fin de asegurararanos que constituyan una base adecuada para reunir ordenadamente la información contable y para preparar los análisis apropiados.

Controles generales.

Si el ASI desea confiar en los controles directos, debe evaluar y probar, cuando corresponda, los controles generales que afectan la confiabilidad de los controles directos clave potenciales. Es importante considerar que un control realizado por un individuo no resultará efectivo si no es realizado cuidadosamente, si es realizado por un empleado que tiene demasiado trabajo o por una persona que no posee la capacidad o el conocimiento necesarios.

Controles de procesamiento y funciones de procesamiento computarizado.

Los sistemas para procesamiento de transacciones de ventas y cuentas por cobrar y su información relacionada generalmente incluye ciertas carateristicas que respaldan directamente las **aserciones** de los componentes de ingresos por ventas y cuentas por cobrar. Estas caracteristicas consisten en controles de procesamiento especificos y funciones de procesamiento computarizado.

5.9.2. Programa de Auditoria para el Rubro de Ventas y Cuentas por Cobrar

La etapa final de la planificación implica la amplificación de los procedimientos de auditoria al agregar los pasos detallados y la organización del trabajo en el orden de ejecución más eficiente. Esta etapa, es denominada: "Preparación de Programas de Auditoria". La planificación generalmente se enfoca a través de tres pasos :

* Consideraciones para la planificación detallada.
* Obtención de información adicional
* Selección de procedimientos de auditoria

5.9.3. Aserciones

Las **aserciones** en los estados financieros son el **eje central** de nuestra evaluación de riesgos y de los sistemas de información computarizados, sistemas contables, de control y para identificar fuentes de satisfacción de auditoria. Cuando se realiza la planificación detallada es importante tener en cuenta las **aserciones** y de qué forma se relacionan con los componentes individuales.

Hay muchas aserciones subyacentes en un juego de estados financieros. Estas aserciones son clasificadas en grupos que son aplicables a todos los componentes. Las aserciones utilizadas en el Programa de Auditoria son los siguientes :

* Estados financieros en su conjunto :

Presentación y Exposición :

Los activos, pasivos y transacciones están correcta y uniformemente resumidos, clasificados y descriptos en los estados financieros. Toda la información necesaria para obtener una adecuada comprensión de los activos, pasivos y transacciones está expuesta en los estados financieros.

* Componentes de los estados financierós :

Veraz :

La empresa es propietaria o posee derechoz respecto de los activos registrados y ha contraído los pasivos contabilizados. Los activos, pasivos y transacciones son reales; los activos existen; las transacciones han ocurrido; las transacciones estan debidamente autorizadas.

Calculado y Valuado :

Las transacciones están correctamente calculadas y reflejadas por su monto apropiado (inluyendo la apropiación a las cuentas correctas y traducción de transacciones en moneda extranjera) y los activos y pasivos estan correctamente valuados, cada uno de acuerdo con su naturaleza y los principios contables aplicables; los activos y pasivos

reflejan todos los hechos y circunstancias que afectan su valuación (incluyendo las variaciones en los tipos de cambio de monda extranjera).

Contabilizado y Acumulado :

Las transacciones, activos y pasivos que deben ser incluídos en los estados financieros están contabilizados. Las transacciones están registradas en la(s) cuenta(s) de acuerdo con su naturaleza y principios contables aplicables, y están registradas en el (o atribuidas al) período contable correspondiente. Las transacciones y saldos individuales están adecuadamente acumulados en los registros correspondientes.

Cuando estos grupos de aserciones están relacionados con componentes individuales, se hacen aparentes las aserciones específicas que son de importancia para el ASI.

Las **aserciones** específicas dentro del grupo de aserciones para el componente de "Ingresos por ventas" para el rubro de ventas y cuentas por cobrar se describen en la página siguiente.

Dichas aserciones son las que aplican en el programa de auditoría diseñado para efectos del caso práctico para el sistemas de ventas y cuentas por cobrar que más adelante se presenta, por medio de estas aserciones muestran al ASI el grado de confiabilidad e integridad de las transacciones; así como el nivel del funcionamiento de los controles tanto manuales y automáticos y el control interno en torno al sistema auditado que está en producción dentro de la organización.

****

VERAZ

HECHO OCURRIDO	* Los ingresos representan montos derivados de la venta de bienes (despacho de bienes y/o transferencia del dominio) y la prestación de servicios; los ingresos están reducidos por las devoluciones y bonificaciones reales y esperadas; las devoluciones y bonificaciones son reales.
AUTORIZADO	* Las condiciones de venta de bienes, prestaciones de servicio, las devoluciones y bonificaciones están adecuadamente autorizadas.

CALCULADO Y VALUADO

MONTO CORRECTO	* Las ventas, descuentos, devoluciones y bonificaciones están correctamente calculados a su monto apropiado de acuerdo con la naturaleza y términos de la transacción y principios contables aplicables.

CONTABILIZADO Y ACUMULADO

CONTABILIZADO	* Todas las ventas están adecuada e íntegramente contabilizadas en los registro correspondientes.
ACUMULADO	* Las ventas están adecuadamente acumuladas en los registros correspondientes.
PERIODO ADECUADO	* Las ventas están registradas en el (o atribuidas al) período adecuado; el corte de operaciones es correcto.

****

INGRESOS POR VENTAS

CARACTERISTICAS DEL SISTEMA QUE RESPALDAN LAS ASERCIONES EN FORMA DIRECTA	ASERCIONES					
INGRESO DE ORDENES DE PEDIDO	HECHO OCURRIDO	AUTORIZADO	MONTO CORRECTO	CONTABILIZADO	ACUMULADO	PERIODO ADECUADO
.El acceso al procesamiento de las órdenes de pedido y de la inclusión de los precios así como a los registros de datos relacionados está restringido.		*	*	*		
.Las listas de precios y los cambios a las mismas son aprobados por un funcionario del nivel apropiado.		*	*			
.Los pedidos son aprobados en cuanto a sus plazos, precios y crédito por un funcionario del nivel apropiado.		*	*			
.Todos los pedidos y datos sobre precios aprobados son ingresados para su procesamiento en forma completa, precisa y sólo una vez.				*		
.Los pedidos y datos sobre precios rechazados son identificados, analizados y corregidos en forma oportuna.				*		*
.El ingreso de pedidos y datos sobre precios es procesado en forma completa y precisa en el período contable correcto, incluyendo la transferencia de datos a otros sistemas.				*		*

INGRESOS POR VENTAS

CARACTERISTICAS DEL SISTEMA QUE RESPALDAN LAS ASERCIONES EN FORMA DIRECTA	ASERCIONES					
DESPACHO DE BIENES Y PRESTACION DE SERVICIOS	HECHO OCURRIDO	AUTORIZADO	MONTO CORRECTO	CONTABILIZADO	ACUMULADO	PERIODO ADECUADO
.El acceso a las funciones de procesamiento de los despachos y las prestaciones de servicios y a los registros relacionados está restringido.		*	*	*		
.Los documentos de despacho que identifican al deudor, cantidades, detalle de los productos y fechas son preparados en forma completa y precisa, sólo sobre la base de pedidos aprobados.	*		*			
.Los documentos de despacho son aprobados por un funcionario del nivel apropiado antes del envío.	*					
.Los documentos de despacho (conocimientos de embarque, remitos) son firmados por los transportistas indicando la aceptación de las cantidades enviadas.	*					
.Los datos sobre todos los despachos de bienes y prestaciones de servicios son ingresados para su procesamiento en forma completa y precisa sólo una vez.	*			*		
.Los datos de despachos o prestaciones de servicios rechazados son identificados, analizados y corregidos en forma oportuna.				*		*
.Los datos de despachos o prestaciones de servicios son procesados en forma completa y precisa en el período contable correcto, incluyendo la transferencia de datos a otros sistemas.				*		*

INGRESOS POR VENTAS

CARACTERISTICAS DEL SISTEMA QUE RESPALDAN LAS ASERCIONES EN FORMA DIRECTA	ASERCIONES					
FACTURACION	HECHO OCURRIDO	AUTORIZADO	MONTO CORRECTO	CONTABILIZADO	ACUMULADO	PERIODO ADECUADO
.El acceso a las funciones de procesamiento de las facturas y notas de crédito y los registros de datos relacionados está restringido.		*	*	*		
.Los bienes despachados y los servicios prestados son facturados con base a las condiciones y precios autorizados.		*	*			
.Todos los datos de las facturas y notas de crédito son ingresados para su procesamiento en forma completa, precisa y sólo una vez.				*		
.Las facturas son preparadas en forma precisa en lo referente al deudor, condiciones, cantidades, precios y cálculos.			*			
.Los datos de las facturas y notas de crédito son conciliados con la documentación de los pedidos, despachos o prestación de servicios y la recepción de bienes devueltos. Las diferencias son investigadas oportunamente.	*		*	*		
.Las facturas o notas de crédito rechazadas o no conciliadas son identificadas, analizadas y corregidas en forma oportuna.	*			*		*
.Los ajustes sobre facturas y notas de crédito son aprobados por un funcionario del nivel apropiado.	*	*				
.Las facturas o notas de crédito son registradas en las cuentas individuales de los deudores.				*		
.Los datos de las facturas y notas de crédito son acumulados en forma completa y precisa en los registros correspondientes.					*	
.Los datos de las facturas y las notas de crédito son procesados en forma completa y precisa en el período contable adecuado, incluyendo la transferencia de datos a otros sistemas.				*		*

INGRESOS POR VENTAS

CARACTERISTICAS DEL SISTEMA QUE RESPALDAN LAS ASERCIONES EN FORMA DIRECTA	ASERCIONES					
PROCEDIMIENTOS ANALITICOS	HECHO OCURRIDO	AUTORIZADO	MONTO CORRECTO	CONTABILIZADO	ACUMULADO	PERIODO ADECUADO
.Revisar los asientos por ventas, devoluciones, descuentos y bonificaciones en las cuentas del mayor general para identificar partidas significativas o inusuales.	*			*	*	*
.Revisar las conciliaciones de las cantidades facturadas con las despachadas, las pedidas y las registradas en el costo de ventas.				*	*	*
.Considerar la razonabilidad global de las ventas multiplicando las unidades vendidas por un precio de venta promedio por producto.	*		*	*	*	*
.Comparar las ventas máximas posibles con las contabilizadas, teniendo en cuenta tendencias estacionales u otras variaciones.	*					
.Las conciliaciones de cantidades facturadas con las despachadas, las pedidas y las registradas en el costo de ventas son revisadas y aprobadas por un funcionario del nivel apropiado.				*	*	*
.Los asientos de ventas y de costo de ventas en el mayor general son conciliados. Las diferencias son investigadas en forma oportuna.				*		*
.Los documentos de despacho, facturas de venta y notas de crédito son prenumerados y los documentos faltantes son investigados en forma oportuna.				*		*
.Las listas de precios y los cambios a las mismas son aprobados por un funcionario del nivel apropiado.		*	*			
.Los pedidos son aprobados en cuanto a sus plazos, precios y crédito por un funcionario del nivel apropiado.		*	*			
.Todas las órdenes de pedidos y datos sobre precios aprobados son ingresados para su procesamiento en forma completa, precisa y sólo una vez utilizando controles de validación.				*		

INGRESOS POR VENTAS

CARACTERISTICAS DEL SISTEMA QUE RESPALDAN LAS ASERCIONES EN FORMA DIRECTA	ASERCIONES					
PROCEDIMIENTOS ANALITICOS	HECHO OCURRIDO	AUTORIZADO	MONTO CORRECTO	CONTABILIZADO	ACUMULADO	PERIODO ADECUADO
.El acceso al procesamiento de las órdenes de pedido y la inclusión de los precios así como a los registros de datos relacionados está restringido utilizando:						
- identificaciones y contraseñas de usuario		*	*	*		
- controles de acceso a terminales		*	*	*		
.Los pedidos y datos sobre precios rechazados son identificados, analizados y corregidos en forma oportuna utilizando:						
- controles de usuario sobre transacciones rechazadas				*		*
- controles de usuario sobre partidas en suspenso				*		*
.El acceso a las funciones de procesamiento de los despachos y de datos relacionados está restringido mediante:						
- identificaciones y contraseñas de usuarios		*	*	*		
- controles de acceso a terminales		*	*	*		
.Los documentos de despacho que identifican al deudor, las cantidades, detalles de los productos y fechas son preparados en forma completa y precisa, sólo sobre la base de pedidos aprobados.	*		*	*	*	*
.Los documentos de despacho son aprobados por un funcionario del nivel apropiado antes de su envío.		*		*		*
.Los documentos de despacho (conocimiento de despacho, remisión) son firmados por los transportistas indicando la aceptación de las cantidades enviadas.	*			*		*
.El último documento de despacho de un período está claramente identificado.						*
.Los datos de todos los despachos de bienes y prestación de servicios son ingresados para su procesamiento en forma completa, precisa y sólo una vez.	*			*		
.Los datos de despacho rechazados son identificados, analizados y corregidos en forma oportuna utilizando:						
- transacciones rechazadas y partidas en suspenso				*		*

INGRESOS POR VENTAS

CARACTERISTICAS DEL SISTEMA QUE RESPALDAN LAS ASERCIONES EN FORMA DIRECTA	ASERCIONES					
PROCEDIMIENTOS ANALITICOS	HECHO OCURRIDO	AUTORIZADO	MONTO CORRECTO	CONTABILIZADO	ACUMULADO	PERIODO APROPIADO
.Los datos de despacho o prestación de servicios son procesados en forma completa y precisa en el período contable correcto, incluyendo la transferencia de datos a otros sistemas, utilizando :						
– procesamiento por lotes				*		*
– controles de transmición de datos				*		*
– controles sobre los datos generados por el sistema				*		*
.El acceso a las funciones de procesamiento de facturas y notas de crédito y a los registros de datos relacionados está restringido utilizando :						
– identificaciones y contraseñas de usuario		*	*	*		
– controles de acceso a terminales		*	*	*		
.Los bienes despachados y los servicios prestados son con base a las condiciones y precios autorizados.		*	*			
.Todos los datos de las facturas y notas de crédito son ingresados para su procesamiento en forma completa, precisa y sólo una vez utilizando controles de validación.				*		
.Las facturas son preparadas en forma precisa en lo referente al deudor, condiciones de pago, cantidades, precios, y cálculos.			*			
.Los datos de las facturas y notas de crédito son conciliados con la documentación de los pedidos, despachos o prestación de servicios, y de la recepción de bienes devueltos. Las diferencias son investigadas :	*		*			
.Las facturas y notas de crédito rechazadas o no conciliadas son identificadas, analizadas y corregidas en forma oportuna utilizando :						
– controles de usuario sobre transacciones rachazadas	*			*		*
– controles de usuario sobre partidas en suspenso	*			*		*
.La exactitud matemática de las facturas y notas de crédito es verificada.			*			

INGRESOS POR VENTAS

CARACTERISTICAS DEL SISTEMA QUE RESPALDAN LAS ASERCIONES EN FORMA DIRECTA	ASERCIONES					
PROCEDIMIENTOS ANALITICOS	HECHO OCURRIDO	AUTORIZADO	MONTO CORRECTO	CONTABILIZADO	ACUMULADO	PERIODO ADECUADO
.Los ajustes de facturas y notas de crédito son aprobados por un funcionario del nivel apropiado.	*	*				
.Los datos de las facturas y notas de crédito son registrados en las cuentas individuales de los deudores.				*		
.Los datos de las facturas y notas de crédito son acumulados en forma completa y precisa en los registros correspondientes.					*	
.Los datos de las facturas y notas de crédito son procesados en forma completa y precisa en el período contable correcto, incluyendo la transferencia de datos a otros sistemas, utilizando :						
- procesamiento por lotes				*		*
- controles de transmisión de datos				*		*
- controles sobre los datos generados por el sistema				*		*

5.10. OBTENCION DE EVIDENCIA

La evidencia es cualquier información usada por el ASI para determinar si la entidad o los datos que están siendo auditados, siguen criterios u objetivos de auditoria establecidos. La evidencia de auditoria puede incluír observaciones del Auditor, notas tomadas, o de resultados de procedimientos de prueba de auditoría. Mientras toda la evidencia ayudará al ASI a desarrollar las conclusiones de auditoría.

5.10.1. Listados y Extracción de Informes

A continuación se detallan los listados e informes generados y los procedimientos de auditoria que se llevaron a cabo durante el seguimiento :

- Existencias de poco movimiento.
- Existencias no recontadas durante el ejercicio.
- Existencias con valor cero.
- Partidas con valor negativo o significativo.

EXISTENCIAS DE POCO MOVIMIENTO

EXISTENCIAS DE POCO MOVIMIENTO

REFERENCIA	VALOR DE LAS EXISTENCIAS	DESCR 2	STOCK DISPONIBLE	CONSUMO ULTIMO AÑO	VALOR DEL FECHA DE DESPACHO
0014263	24 680 23	Rueda	92	4	84 352
0011607	*69 465 23	Derivacion	21	1	84 237
001426*	28 305 80	Rueda	136	15	84 244
0026626	*4 488 32	Rueda	56	0	83 284
0026557	24 715 58	Anillo	864	84	85 222
0025586	14 052 90	Ventilador	6	0	84 138
0023331	51 723 50	Horquilla	291	21	84 269
0140429	* 548 907 50	Riel	29 503	3	84 195
0140168	893 178 00	Riel	11 451	*5	85 262
0151939	14 405 40	Polea	200	0	84 219
0172496	102 016 47	Junta	217	4	85 262
0177015	13 475 00	Cilindro de propano	350	0	78 000
0186853	85 47* 85	Kit	2 350	0	85 195
0118986	166-*51 68	Almohadilla	1 312	97	85 268
0118987	574 523 20	Almohadilla	3 740	0	84 162
0243405	58 650 00	Kit	170	0	85 251
TOTAL	3 784 210 66				

EXISTENCIAS NO RECONTADAS DURANTE EL EJERCICIO

EXISTENCIAS NO RECONTADAS DURANTE EL EJERCICIO

REFERENCIA	VALOR DE LAS EXISTENCIAS	DESCR 2	UBICACION FISICA DEL STOCK	STOCK DISPONIBLE	CONSUMO ULTIMO AÑO
0020828	24 018 47	Eje	A-2-A	20	31
0023331	5' *23 50	Horquilla	STL Playón	291	221
0025586	14 052 80	Ventilador	74AB03AA	6	0
0026557	24 715 58	Anillo	*7AH01AA	864	784
0026637	18 988 *0	Zapata	Rampa-1	2 700	15 433
0026626	14 488 32	Rueda	Playón	56	0
0014261	26 305 80	Rueda	STL Playón	136	115
0014263	25 680 23	Rueda	Playón	82	444
0014264	107 243 53	Rueda	STL Playón	428	2 720
0014265	72 594 28	Rueda	STL-Playón	234	307
0187445	214 192.00	Unión	Playón	13 387	30 514
0188853	85 471 85	Kit		2 350	0
0177015	13 475 00	Cilindro de propano	Playón	350	0
0151939	14 405 40	Polea	Playón	200	0
0163055	1 409 318 97	DFG-2	Taller	2 898 551	12.179 858
0118986	166 *51 68	Almohadilla	Playón	1 312	297
0126324	29 787 12	Cabezal	STL-Playón	36	299
0118987	574 523 20	Almohadilla	Playón	2 740	0
0126482	11 131 28	Placa	STL-Playón	129	383
0131951	110 354 10	Cupla	Playon	219	509
0114620	16 862.39	Guia	R-1802	1	1
0114619	16 862.39	Guia	R-1802	1	1
0243405	58 850 00	Kit	Playón	170	0
TOTAL	3 10* 195.99				

EXISTENCIAS CON VALOR CERO

EXISTENCIAS CON VALOR CERO

REFERENCIA	VALOR DE LAS EXISTENCIAS	UBICACION	DESCR 2	PRECIO	POH	FECHA ULTIMO DESPACHO
0010996	0 00	03AE23FA	REGULADOR	0 000	1	84 029
0010958	0 00	03AE23BA	REGULADOR	0 000	1	78 000
0010993	0 00	04DA07BA	REGULADOR	0 000	1	78 000
0010935	0 00	25AB06HA	GENERADOR	0 000	1	78 000
0010938	0 00	16DC07BA	ARRANCADOR	0 000	2	84 205
0010953	0 00	25AB06BA	GENERADOR	0 000	1	78 000
0010956	0 00	07DA07CA	REGULADOR	0 000	1	81 345
0010929	0 00	25AB06HA	ARRANCADOR	0 000	1	78 000
0010677	0 00	19AG06CA	REFRIGERADOR	0 000	1	85 146
0010931	0 00	15BB07AA	ARRANCADOR	200 000	1	78 000
0010933	0 00	25AH07AA	ARRANCADOR	0 000	1	82 329
0010676	0 00	30 6 8	INYECTOR	0 000	2	78 040
0010493	0 00	01CA01FJ	SELLO	0 000	1	78 000
0010430	0 00	05RG17CA	BOMBA	0 000	1	79 064
0010447	0 00	21AA05BA	BLOCK	0 000	2	82 126
0010424	66 60	01CD08EA	SEPARADOR	66 600	2	85 017
0010303	0 00	RK-114	BOMBA	0 000	1	79 062
0010420	44 50	05CI07CA	SEPARADOR	44 500	4	85 017
0010297	0 00	RK-114	BOMBA	0 000	1	79 962
0010183	0 00	RK 93-T	BASTIDOR	0 000	8	78 000
0011026	0 00	04AE22DA	MAGNETO	0 000	2	85 012
0011007	0 00	05CC20EA	REGULADOR	0 000	1	84 203
0011011	0 00	03AD23FA	REGULADOR	0 000	1	81 036
0011012	0 00	16BC07BA	GENERADOR	0 000	2	82 308
0011013	0 00	16AJ08BA	REGULADOR	0 000	1	79 068
0020828	24 018.47	A-2-A	EJE	1 264 130	20	85 157
TOTAL	24 129.57					

DATOS DEL PROGRAMA UTILITARIO
ITEMS CON VALOR NEGATIVO O SIGNIFICATIVO

NO REPUESTO	DESCRIPCION	UNIDAD	CANTIDAD	VALOR UNITARIO	VALOR TOTAL DE LAS EXISTENCIAS
0374890	TIRANTES, 7 x 9 x 9 PIES	7	26 774	32,00-	856 768,00-
0229238	CAJA DE CAMBIOS, SUPERIOR	7	2-	,00	,00
0187445	TIRANTES, 7 x 9 x 9 PIES	9	13 387	16,00-	214 192,00-
0114619	CAJA DE CAMBIOS, SUPERIOR	7	1-	,00	,00
0093722	TIRANTES, 7 x 9 x 9 PIES	10	6 693	8,00-	53 544,00-
0021986	REGULADORES, REPARADOS	7	2-	,00	,00
0020840	SEPARADORES, AIRE ACON	7	8	83,00-	664,00-
0020228	MOTOR, LIMPIAPARABRISAS	7	6-	83,58	501,48-
0010993	REGULADORES, REPARADOS	4	1-	,00	,00
0010420	SEPARADORES, AIRE ACON	3	4	41,50-	166,00-
0010114	MOTOR, LIMPIAPARABRISAS	1	3-	41,79	125,37
0005210	SEPARADORES, AIRE ACON	3	2	20,75-	41,50-
0005057	MOTOR, LIMPIAPARABRISAS	1	1-	20,89	20,89-
0280858	RIELES, CHATARRA (TONELADAS)	7	59 008	124,00	7 316 744,00
0326110	ACEITE	7	957,102	5,39	5 158 779,78
0064658	RIELES RECTOS, 132 Libras	7	4 960	604,86	3 012 702,80
0280336	RIELES, RELE (TONELADAS)	7	22 902	124,00	2 839 848,00
0237974	ALMOHADILLAS MF-275-1	7	5 480	351,12	1 924 137,60
0140429	RIELES, CHATARRA (TONELADAS)	8	29 503	62,00	1 924 137,60
0163055	ACEITE	8	998 551	1,29	1 288 130,79
0032329	RIELES RECTOS, 132 Libras	7	2 490	302,43	753 050,70
0140168	RIELES, RELE (TONELADAS)	8	11 451	62,00	709 962,00

INFORME	PROCEDIMIENTOS DE SEGUIMIENTO
Existencias por sección.	Comparamos los valores de existencias con los montos del mayor general. Asegurarnos de que el informe concuerda con nuestro entendimiento de la actividad de cada sección.
Comparación del costo unitario con el último precio pagado.	Examinamos cuidadosamente la valuación del artículo No. 1404220 y consideramos la necesidad de ajustar el precio estándar (diferencia significativa con el último precio pagado).
Partidas de poco movimiento.	Consideramos la necesidad de desvalorizar estas partidas. Revisamos el listado de existencias de poco movimiento de la gerencia e investigamos las razones por los eventuales casos de existencias no listadas por el programa.
Existencias no recontadas.	Consideramos la inclusión de los materiales significativos durante el ejercicio en las pruebas de recuento físico. Investigamos las razones que por éstos artículos aún no han sido recontados.

INFORMES	PROCEDIMIENTOS DE SEGIMIENTO
Listado de ajustes significativos de existencias.	Modificamos el programa para que cuente y sume todos los ajustes de existencias, separando los ajustes positivos de los negativos. El programa identificó sólo los ajustes positivos superiores a $1,000.
Mercancía recibida pero no facturada	Comprobamos la provisión por este concepto lo cual es correcto.
Existencias negativas.	Nos aseguramos de que el informe imprime los productos cuyo saldo de existencias es negtivo. Investigamos los saldos negativos significativos.
Existencias con valor cero.	Investigamos por qué éstos materiales no se venden como rezago, conservamos el informe para comprobar que al año siguiente no se les asigne un valor.
Precio de despacho distinto al precio de compra	Nos asegurarse de que se calcula correctamente el costo estandar, tomando en cuenta las diferentes unidades de medida que se utilizan.

5.11. RESULTADOS

5.11.1. Conclusión

Como resultado del seguimiento sobre los datos resultantes se generaron recomendaciones a la gerência tendientes a eliminar una ruta defectuosa del programa de ventas y cuentas por cobrar que había dado lugar a la aparición de existencias negativas y a incrementar la frecuencia de los recuentos cíclicos de partidas de alto valor.

La Gerencia de la Compañia, con base a los reportes entregados, decidió preparar informes mensuales de existencias.

En conclusión, si bien el programa de recuperación y análisis fue más costoso durante el primer año de aplicación que las técnicas mensuales alternativas, el retorno sobre la inversión representado por la identificación de problemas potenciales (que eventualmente podrían haberse vuelto importantes) fue satisfactorio, asimismo, se espera alcanzar en dos años el punto de equilibrio entre el costo del programa y el costo del tiempo insumido en las tareas menuales. De tal forma, actualmente las entradas, los procesos y salidas de información en el sistema de ventas y cuentas por cobrar en operación no presenta debilidades importantes que pudiran interrumpir la continuidad de las operaciones, asi como la integridad y confiabilidad de los datos y salvaguarda de activos **son correctos**, cumpliendo con los objetivos de control gerencial.

5.12. REPORTES DE AUDITORIA DE SISTEMAS

Los reportes de Auditoría son el producto final del ASI. Este es el vehículo que el ASI usa para reportar hallazgos y recomendaciones a la Administración. El ASI debe entender las normas generales de EDPAF No. 9 "Reporte de cobertura de Auditoría y el No. 10 "Reporte de hallazgos y conclusiones".

5.13. ACCIONES DE LA ADMINISTRACION PARA IMPLANTAR LAS RECOMENDACIONES

Los ASI deben darse cuenta que auditar es un proceso progresivo. La auditoría no cumple su objetivo si no hay seguimiento para determinar si las acciones correctivas prometidas han sido tomadas bajo las recomendaciones de la auditoría. El tiempo del seguimiento dependerá de lo crítico de los hallazgos y estarían sujetos al juicio del ASI.

Los resultados del seguimiento deben ser comunicados a los niveles de administración apropiados.

CONCLUSION

Durante el desarrollo del presente trabajo, se ha encontrado que la Auditoría Informática es una herramienta esencial en la administración de los sistemas de información computarizados, ya que permite la evaluación de los controles, su planteamiento y adecuación a las necesidades específicas del sistema.

La metodología expuesta, se encuentra desarrollada para sistemas que utilizan algún tipo de procesamiento electrónico de datos, y que éste haya sido diseñado bajo los lineamientos especificos de la Aditoría en Informática. Su aplicabilidad parte del hecho que el sistema es auditable y que éste contiene los elementos mínimos necesarios de control en operación a ser evaluados.

El presente trabajo, en su conjunto, integra elementos que se consideraron como básicos y que el auditor habrá de conocer. Se describieron conceptos, en algunas ocasiones en forma sintética, como; el control, los sistemas, la seguridad de los sistemas de información y las condiciones de riesgo, de tal manera que sus cuestionamientos sobre la aplicación de la metodología le sean más claros al encontrarse con estos conceptos. No debe olvidarse que el ASI es un elemento importante en el éxito de la aplicación de cualquier metodología y que de su apreciación y experiencia depende el llegar a buen término. La metodología fué desarrollada con base a Descripción, Evaluación, Verificación, Comprobación, Presentación de Resultados y Seguimiento, ya que esto determina las posibilidades de auditar el sistema, por lo que permite el ahorro de recursos en la aplicación de un programa de auditoría, dado que no habra que aplicar todo el proceso de la metodología para el caso que un sistema no contenga los elementos mínimos necesarios para realizarlo.

Se consideró que la metodología deberá concluirse con el establecimiento de un programa de auditoría a corto y mediano plazo que garantice su retroalimentación con el sistema y que se tenga de ésta, la participación directa e indirecta de los integrantes del sistema, del conocimiento del sistema y de la operatividad de los controles actualmente instalados. Los resulados no serán observados de forma inmediata dado que habrá de esperar un ciclo completo, donde los resultados de la auditoría han sido implementados y regulando los controles del sistema.

BIBLIOGRAFIA

AGUIRRE Martínez Eduardo, Seguridad Integridad en las Organizaciones : actualización para ejecutivos, Edit. Trillas, México., 1980, Pp. 720.

ARTHUR Andersen & Co., FAST I, Escuela de Entrenamiento en Auditoría, Vol. I y II, USA, 1990, Pp. 260.

ARTHUR Andersen & Co., FAST II, Escuela de Entrenamiento en Auditoría, Vol. I y II, USA, 1990, Pp. 350.

BANK Administration Institute, Auditing the Systems Development Life Cycle, Rolling Meadows, USA, 1979, Pp. 42.

BURCH, John., Computer Control and Audit, John Wiley & Sons, New York, USA, 1978, Pp. 130.

COLEGIO de Contadores Públicos, Diferentes enfoques de Auditoría en Informática, México, 1991, Pp. 370.

ELECTRONICAL Data Processing Auditors Foundation (EDPAF), Inc., CISA Review Manual, Domian 7, USA, 1992, Pp. iii-1.

FINE Leonard H., Seguridad en Centros de Cómputo, Edit. Limusa, México, 1983, Pp. 130.

GEREZ, V., MIER, M., Desarrollo y Administración de Centros de Cómputo, Instituto de Investigaciones Eléctricas, C.E.C.S.A., México, 1985,Pp. 280.

GORDON B., Davis, La Auditoría y el Procesamiento Electrónico de Información, Instituto Mexicano de Contadores Públicos, México, 1992, Pp. 347.

GUIA para la elaboración de estudios de viabilidad sobre sistemas de computación, varios autores, S.P.P., México, 1981, Pp. 120.

INSTITUTO Mexicano de Auditores Internos Manual del Seminario : Auditoría en Sistemas, México, 1987, Pp. 180.

INSTITUTO Mexicano de Contadores Públicos, Normas y Procedimientos de Auditoría, Novena Edición, México, 1989, Pp. 240.

INSTITUTO Mexicano de Contadores Públicos, Procedimientos de Control en Computación, México, 1987, Pp. 290.

JANCURA, Elise and Arnold Berger, Computers : Auditing and Control, Auerbach Publishers, USA, 1973, Pp. 420.

KOHLER, Eric L., Diccionario para Contadores, Edit. Limusa, México, 1992, Pp.520.

LEONARD, William., Auditoría Administrativa, Edit. Diana, México, 1984, Pp.350.

LOTT, Richard., Auditoría y Control del Procesamiento de Datos, Edit. Norma, Colombia, 1984, Pp. 330.

MAIR, William., WOOD, Donald,. Auditoria y Control del Computador, Instituto Mexicano de Contadores Públicos, Grpo. Edit. Printamatic S.A., México, 1976, Pp. 380.

MAIR, William, Computer Control & Audit, The Institute of Internal Auditors, USA, 1978, Pp. 320.

MANUAL del Estudiante, Administración de Centros de Cómputo, Honeywell Sistemas de Información, México, 1986, Pp. 180.

PRICE Waterhouse, El Proceso de Auditoría para Desarrollar Programas de Auditoría, New York, USA, 1971, Pp. 420.

PRICE Waterhouse, La Auditoría en un Ambiente de Procesamiento Electrónico de Información, Fascículo II, México, 1972, Pp. 43.

PRICE Waterhouse, Revisión del Procesamiento Electrónico de Información, New York, USA, 1971, Pp. 340.

PRICE Waterhouse, Sistemas de Información Computarizados, Serie de Guías de Auditoría, Guía Complementaria, Buenos Aires, Argentina, 1988, Pp. 400.

SANDERS E., Donald, Informática : Presente y Futuro, Edit. McGraw Hill, México, 1985, Pp. 420.

SCHAEFFER, Haward., Data Center Operations : A Guide to Effective Planning, Processing and Performance, Edit. Prentice Hall, USA, 1981, Pp. 380.

SLOSSE, Carlos, ET. al., Auditoría, Un nuevo enfoque Empresarial, Edit. Ediciones Macchi, segunda edición, Buenos Aires, 1989, Argentina, Pp.1113.

THORIN, Marc, La Auditoría en Informática, Masson, México, 1980, Pp. 79.

WEBER, Ron EDP Auditing, Conceptual Foundations and Practice, Edit. McGraw Hill, second edition, USA, 1989, Pp. 990.