UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

"AUDITORIA EN INFORMATICA"

SEMINARIO DE INVESTIGACION EN INFORMATICA

QUE EN OPCION AL GRADO DE :

LICENCIADO EN INFORMATICA

P R E S E N T A N :

CASTAÑEDA VIVAR ROSALIA

SCHULZ ZEPEDA ROLANDO

DIRECTOR DE SEMINARIO:
L.A.E. Y M.B.A. JOSE ANTONIO ECHENIQUE GARCIA

MEXICO, D.F. 1991

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

INDICE

INTRODUCCION

INTRODUCCION

La auditoría en informática es una función que ha sido desarrollada para asegurar si los sistemas salvaguardan activos, mantienen la integridad de datos y logran los objetivos de una organización efectiva y eficientemente. Tanto las partes internas y externas de una organización se concentran en que los sistemas cumplan por completo esos objetivos. De este modo la auditoría en informática soporta el logro de los objetivos de auditorías tradicionales: objetivos de certificación (para un auditor externo) que hacen énfasis en la salvaguarda de activos e integridad de datos y objetivos gerenciales (para un auditor interno) que se enfocan 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.

Salvaguarda de activos. Los activos de una instalación de cómputo incluyen hardware, software, personal, archivos de datos, documentación de los sistemas y papelería. Como todos los activos, deben ser protegidos por un sistema de control interno. Debido a la concentración de activos en un centro de cómputo, la salvaguarda de activos es un objetivo muy importante.

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 y coherencia. Si la integridad de datos no es mantenida, una organización ya no cuenta con una representación de si misma o de lo eventos del mundo real. Sin embargo la integridad de datos solo puede ser lograda a un costo. Los beneficios obtenidos deben exceder el costo del procedimiento de control requerido.

Dos factores principales afectan el valor de un elemento de información de una organización: (a) el valor del contenido de información del elemento para tomadores de decisiones individuales y (b) el grado en que el elemento de datos es compartido entre tomadores de decisiones. El valor del elemento determina que tan importante es mantener la integridad del elemento de datos.

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 un sistema reporta información en 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 ocurre por lo general después de 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.

Eficiencia del Sistema. Un sistema de procesamiento de datos eficientes utiliza los 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 incógnita es, si un sistema de procesamiento de datos es eficiente, aunque por lo general nunca llega a ser resuelta. La eficiencia de 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. La eficiencia de un sistema de procesamiento de datos pasa a ser importante cuando una computadora ya no cuenta con exceso de capacidad.

Para cumplir con estos objetivos, trazamos el siguiente capitulado a fin de establecer parámetros y procedimientos que guien al auditor en la consecusión de los mismos:

I. Auditoría de Sistemas. Donde se tratan los conceptos de auditoría y sus divisiones, concepto de auditoría en informática, metodología de una auditoría, código de ética y normales generales que pueden adoptarse por el auditor; todo ello con el fin de establecer un punto de arranque y la estandarización de los términos a utilizar.

II. Controles y Riesgos en un Ambiente de Sistemas Automatizado. Durante el desarrollo se muestran los posibles riesgos existentes en un ambiente automatizado de sistemas y los posibles controles que al establecerse minimizarían la probabilidad de ocurrencia.

III. Planeación de la Auditoría en Informática. Donde se conocerán los puntos que son necesarios cubrir para determinar el tamaño y características del área dentro de la organización a auditar, la complejidad de sus sistemas, organización y equipo, con lo cual podremos definir los alcances de la auditoría, las herramientas necesarias, el tiempo y el costo de la realización.

IV. Seguridad en un Centro de Cómputo. Durante su desarrollo se analizarán y evaluarán las políticas y procedimientos operativos y controles de acceso usados para proteger los activos informáticos. Así mismo se expondrán procedimientos concernientes a la planeación de contingencias para asegurar la continuidad de operaciones en caso de desastre.

V. Sistemas de aplicación. Donde se evaluarán los controles de aplicación a las funciones de entrada de datos, proceso y salida de información, tratando de establecer el nivel de confianza a depositar en cada uno de ellos a fin de que se asegure la obtención óptima del objetivo trazado para un determinado sistema.

VI. Obtención, Evaluación de Evidencia y Reporte de Auditoría. Donde se muestra la forma propuesta de presentación de resultados de la auditoría y su presentación hacia el ente auditado, considerando el seguimiento que debe existir del cumplimiento de las observaciones presentadas.

CAPITULO I

AUDITORIA DE SISTEMAS

I. AUDITORIA DE SISTEMAS

OBJETIVO

- Conocer los tipos de auditoría existentes.
- Entender los componentes de una auditoría.
- Conocer los principios de auditoría de sistemas.

INTRODUCCION

Se requieren varios pasos para realizar una auditoría. El auditor en informática debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos. El proceso de auditoría exige que el auditor en informática reúna evidencia, evalúe las fortalezas y debilidades de controles basados en la evidencia recopilada, y que prepare un informe de auditoría que presente estos temas de auditoría en forma objetiva a la gerencia. Asimismo, la gerencia de auditoría debe garantizar una disponibilidad y asignación adecuadas de recursos de auditoría para realizar la auditoría además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia. Los auditores en informática también deben tener un adecuado conocimiento tanto del código de ética y las normas profesionales de la EDPAF.

1. CONCEPTO DE AUDITORIA

La auditoría ha sido conceptualizada y definida de diversas maneras, por lo que a continuación se presentan algunas definiciones representativas por medio de las cuales podremos comprender la razón de una auditoría a un centro de cómputo y a los sistemas de información.

Auditoría

'Es la revisión de cualquier actividad que sea susceptible de control'.

Auditoría

'Es un proceso sistemático para obtener y evaluar de manera objetiva la eficiencia y la eficacia con que se está operando sobre actividades económicas, técnicas y sociales, y otros acontecimientos relacionados para que por medio del señalamiento de cursos alternativos de acción, tomar decisiones que permitan corregir los errores (en caso de que existan) o bien mejorar la forma de actuación'.

2 CLASIFICACION DE LA AUDITORIA

Una organización siempre se encuentra en desarrollo, creando nuevos aspectos, por lo cual se propician cambios en organizaciones. Es por ello, que las necesidades de la auditoría se amplían, creando nuevos campos de aplicación, razón por la cual la EDAD (Asociación de Auditores al Proceso Electrónico de Datos) clasifica a la auditoría como sigue:

1. Auditoría Financiera

El propósito de la Auditoría Financiera, es asegurar la validación de los estados y registros financieros. Una auditoría financiera frecuentemente lleva consigo pruebas de detalle y sustantivas. El auditor en sistemas con frecuencia utiliza procedimientos asistidos por el computador para apoyar a los auditores financieros en la auditoría.

2. Auditoría Operacional

Una auditoría operacional esta diseñada para evaluar la estructura de control interno en un área dada, muchos auditores en sistemas de información, incluyen la revisión de los controles de aplicación o de seguridad lógica de sistemas, que son de naturaleza operativa.

3. Auditoría Integral

Una auditoría integral combina pasos de la auditoría financiera y de la operacional. Una auditoría integral incluye pruebas de cumplimiento y sustantivas.

Los programas de auditoría financiera, operacional e integral deben seguir los mismos procedimientos, así como pasos para cualquier auditoría, sin embargo, los resultados esperados en cada paso pueden ser diferentes.

Por otro lado, es importante mencionar que la auditoría puede clasificarse de acuerdo a la periodicidad con que se lleve a cabo en:

a) Continua o Permanente

Es aquella revisión que se practica de modo continuo a medida que se llevan a cabo las operaciones, o a intervalos cortos y regulares poco tiempo después de efectuadas al terminar el período de concentración, que es cuando pueden evidenciarse las operaciones que usualmente tienen como objetivo facilitar la Auditoría de Estados Financieros a la terminación del ejercicio.

b) Esporádica

Esta auditoría se lleva a cabo en cualquier tiempo, ya sea detalladamente o mediante pruebas selectivas y llevadas a cabo para examinar aisladamente alguna o algunas áreas de la organización.

c) Periódica

Es aquella que se practica cada cierto tiempo dentro de un mismo ejercicio, ya sea en detalle o por medio de pruebas selectivas, generando informes parciales al dictamen sobre Estados Financieros al finalizar el ejercicio.

Ahora bien, en función a la relación que guarda el auditor con la empresa en la cual se desarrolla la auditoría, podemos dividirla en:

Auditoría Interna

Es cuando la auditoría es llevada a cabo por empleados de la organización, cuyos procedimientos e informes están siendo revisados. Dentro de la organización, los auditores internos deben ser independientes de aquellos cuyos trabajos revisan. Ocupan una posición de asesoría y deben presentar sus informes directamente a alguien en las áreas administrativas mas altas de la misma. Los auditores internos llevan a cabo una función importante dentro de las empresas mercantiles, dependencias gubernamentales y otras formas de organización. Al revisar el sistema de información interna el auditor interno determina si el sistema ha sido diseñado de manera efectiva para comunicar las instrucciones de la Dirección, recopilar la información necesaria e informar a la Dirección los resultados de las actividades de las operaciones. Esta revisión en consecuencia consiste en la evaluación del sistema implantando observaciones sobre el funcionamiento del mismo y recomendaciones sobre su mejora.

Auditoría Externa

Es aquella que se lleva a cabo por profesionistas independientes, cuyos servicios pueden ser solicitados por una organización para analizar sus sistemas de información y presentar un informe de auditoría que exprese su opinión acerca del adecuado funcionamiento de la organización. Dicho informe no está desviado por las necesidades o deseos de algún grupo miembro de la organización en particular. La característica fundamental de un auditor externo es la independencia de actitud mental, la integridad y la objetividad. Cabe señalar que el informe de

auditoría reviste un carácter legal, contrariamente a la Gerencia General, el auditor no es responsable de la detección de fraudes.

3 NORMAS DE AUDITORIA

Como hemos mencionados, la auditoría tiene como función el evaluar y revisar el control interno de una organización lo cual implica el ejercicio de una actividad especializada y la aceptación de una responsabilidad pública, para lo cual es necesario contar con guias de acción de carácter prudencial a las que debe de sujetarse, mismas que son conocidas como Normas de Auditoría.

Podemos definir a las Normas de Auditoría como los requisitos mínimos de calidad relativos a la personalidad de un auditor, al trabajo que desempeña y a la información que rinde como resultado de dicho trabajo. Dichas Normas son:

Relativas al desempeño del trabajo:

1. Planeación adecuada del trabajo.
2. Estudio y Evaluación del Control Interno.
3. Suficiencia en la evidencia comprobatoria.

Relativas a la personalidad:

1. Independencia en su actitud mental.
2. Capacitación.

4 AUDITORIA EN INFORMATICA

Es la revisión y evaluación de los controles, sistemas y procedimientos, involucrados en el procesamiento de la información, para que por medio del señalamiento de cursos alternativos, se logre una utilización más eficiente y segura de la información que sirve para una adecuada toma de decisiones.

La Auditoría en Informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistema o procedimiento específico, deberán evaluarse los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información. Lo cual debe involucrar a los equipos de cómputo, departamento de información adecuado y a la organización específica (departamento de cómputo, departamento de informática, gerencia de procesos electrónicos, etc.) que hará posible el uso de los equipos de cómputo.

AREAS DE APLICACION

a) Auditoría a la estructura funcional del área de sistemas. Esta área se orienta hacia la Gerencia General considerando los controles administrativos desde el punto de vista de la Alta Gerencia tomando en cuenta el área de sistemas como un ente independiente y como un ente integral de la organización.

b) Auditoría al desarrollo de sistemas. Esta área se orienta al análisis, desarrollo y mantenimiento de sistemas. La evaluación sigue generalmente el ciclo de vida del desarrollo de sistemas tales como planeación, organización y control de las actividades de procesamiento de datos.

c) Auditoría al área de operaciones. Esta área se orienta a la evaluación de un centro de cómputo, tomando en cuenta asuntos relacionados a control de acceso, seguridad física, respaldo y recuperación.

d) Auditoría sobre aplicaciones. Esta área se orienta hacia programas de aplicación, se evaluan puntos que van relacionados con la integridad de los datos desde su origen para entrada, su proceso y hasta su salida.

5 METODOLOGIA EN LA AUDITORIA EN INFORMATICA

El objetivo es garantizar que el auditor en informática se apegue a las normas, y al uso adecuado de procedimientos y técnicas comunes en el desarrollo

de auditorías. El auditor deberá entender los pasos y técnicas necesarias para planear, desempeñar y completar una auditoría.

Cuando se cumple con las normas y procedimientos de auditoría, las tareas del auditor deberán incluir lo siguiente:

- Planear un enfoque de auditoría eficiente y efectivo, definiendo los objetivos y el alcance de la misma, preparando el programa y planeando los recursos necesarios para su desarrollo.

- Obtener y documentar las pruebas de auditoría, utilizando las técnicas apropiadas.

- Evaluar las fortalezas y debilidades del área bajo auditoría para informar de su efectividad, eficiencia y el estado de los controles.

- Escribir y presentar un informe de hallazgos, conclusiones y recomendaciones para informar a la administración de la suficiencia de controles y la efectividad de las operaciones.

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

5.1 Planeación

La planeación adecuada es el primer paso en la realización efectiva de las auditorías en informática. El auditor deberá entender el entorno general de la empresa, donde la auditoría va a ser realizada, así como los riesgos de la empresa asociados. Las siguientes son parte de las áreas que deberán ser cubiertas durante la planeación de la auditoría.

5.1.1 Entender la Empresa y su Medio Ambiente

Cuando se planea una auditoría, el auditor deberá tener una comprensión general del medio ambiente bajo

revisión. Está deberá incluir un entendimiento general de las diversas actividades de la empresa y funciones referentes al tema de auditoría. El auditor necesita también entender el entorno regulador en el cual opera la empresa.

Los pasos que un auditor podría seguir para obtener una comprensión de la empresa pueden incluir:

- Leer material retrospectivo, incluyendo publicaciones, informes anuales, preinformes de análisis financieros, entre otros.
- Entrevistar a los principales Directores para entender las actividades de la empresa.
- Revisar previamente los informes de auditoría y los planes estratégicos a corto y largo plazo.
- Leer material sobre el comité de sistemas.
- 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.

5.1.2 Riesgos de Auditoría y Materialidad

El riesgo de auditoría puede ser definido como el riesgo de que la información pueda contener un error material que el auditor no pueda detectar un error que ya haya ocurrido. El riesgo de auditoría 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 basado en el sistema de control interno.
- Riesgo de detección. Es el riesgo que un auditor tiene al realizar pruebas exitosas de un procedimiento de análisis inadecuado. El auditor

puede concluir 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 debe 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 a sistemas de información la definición de un error material dependerá del tamaño o importancia de la entidad bajo auditoría, así como de otros factores.

5.1.3 Objetivos de Control Interno

Un sistema automatizado bien diseñado deberá tener controles internos sobre todo en sus principales funciones. Además el auditor en informática entenderá los objetivos de control básicos que deberán existir para todas las aplicaciones. Los componentes 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 diarias cumplan con los objetivos de la empresa.

- Controles administrativos.- Son establecidos de-acuerdo con la eficiencia operacional en el área funcional. Los controles 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.

5.1.4. 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 auditor debe tomar los objetivos de control interno y trasladarlos hacia procedimientos específicos de auditoría en informática.

Algunos ejemplos de objetivos de control interno automatizados incluyen:

- Cada transacción debe ser capturada y actualizada solo una vez.
- Todas las transacciones reprocesadas deben ser reportadas.
- Las transacciones duplicadas deben reportarse.
- Los archivos deben debidamente ser respaldados para permitir una recuperación adecuada.
- Todos los cambios a la operación del software deben ser aprobados y evaluados.

5.1.5 Objetivos de la Auditoría a 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 auditor en informática debe 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.

5.1.6 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 seguridad razonable 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 utilización de documentos y registros adecuados, a fin de ayudar a asegurar el correcto registro de transacciones (ejemplo: pista de auditoría de transacciones).

- Procedimientos y funciones para asegurar el acceso y uso adecuados las instalaciones y equipo.

- Políticas de seguridad física que se apliquen a todos los centros de cómputo.

Esta lista puede ser aumentada, sin embargo, el auditor debe entender estos conceptos generales de procedimientos de control y como aplicarlos en la planeación de una auditoría.

Los controles son generalmente definidos en tres clasificaciones principales:

- Preventivos

  Son aquellos controles que están diseñados para prevenir la ocurrencia de un error, omisión o acto malicioso.

- Detectivos

  Son aquellos controles que detectan un error, omisión o acto malicioso que ha ocurrido y que se ha reportado la ocurrencia.

- Correctivos

Son quellos controles que corrigen los errores, omisiones o actos maliciosos, una vez que se han detectado.

5.1.7 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 auditor puede relacionar el procedimiento general de un respaldo a un sistema de información, 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.
- Metodología en el desarrollo de sistemas.
- Operación de procesamiento de datos.
- Programación de sistemas y funciones de soporte técnico.
- Procedimientos que aseguren la calidad del procesamiento de datos.

El auditor debe entender como los procedimientos de control general pueden ser trasladados a otros más específicos de control de sistemas de información.

5.1.8 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 la auditoría,
- Revisión preliminar del área o sujeto de auditoría,
- Obtener, registrar y entender al área o sujeto de auditoría,
- Evaluar el área o sujeto de auditoría,
- Prueba de cumplimiento,
- Prueba sustantiva,
- Reporte de auditoría, y
- Seguimiento.

5.1.9 Procedimientos de Auditoría en Informática

Las auditorías en informática 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 debe entender los procedimientos de prueba y evaluación de los controles de los sistemas de información, estos procedimientos incluyen:

- El uso de software generalizado de auditoría para examinar el contenido de los archivos de datos.
- El uso de software especializado para evaluar el contenido de los archivos de datos.
- Técnicas de diagramas de flujo para documentar aplicaciones automatizadas.

El auditor en informática debe tener suficiente entendimiento de estos y otros procedimientos para permitir la planeación de pruebas de auditoría apropiadas.

El auditor dede identificar que otras consideraciones pueden impactar en el rendimiento general de la auditoría y tomar en cuenta tópicos tales como:

- La implantación de sistemas.
- Tecnologías actuales y futuras.
- Limitación de los recursos de los sistemas de información.

5.2 Desarrollo de Programas de Auditoría

5.2.1 Estructura y Fases del Programa de Auditoría

Un programa de auditoría es un grupo de procedimientos de auditoría documentados y diseñados para cumplir con los objetivos de auditoría planeados. Un programa típico de auditoría debe incluir lo siguiente:

- Sujeto de auditoría
  - . Identificar el área a auditar
- Objetivo de la auditoría
  - . Identificar el propósito de la auditoría.
- Alcance de la auditoría
  - . Identificar los sistemas específicos o la unidad de la organización a ser incluída en la revisión.
- Planeación de la 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 a ser auditados.

- Procedimientos y Pasos de Auditoría:

. Reunir datos

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

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

. Desarrollar herramientas y metodologías de auditoría pata evaluar y verificar los controles.

- Procedimientos para examinar los resultados de pruebas o 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 auditor debe firmar y fechar los diversos pasos, tal como los realice para proporcionar una pista de registro y realización.

Aunque un programa de auditoría no sigue necesariamente un grupo de pasos, el auditor en informática debe seguir la secuencia de fases del programa para obtener una comprensión de la entidad bajo auditoría, evaluar la estructura de control, y entonces examinar los controles.

5.2.2 Prueba de Cumplimiento vs Prueba Sustantiva

La diferencia entre la prueba de cumplimiento y la prueba sustantiva es un concepto importante para el auditor. Una prueba de cumplimiento determina si los controles están siendo aplicados, de la manera indicada en la documentación del programa o como se describe por el auditado. Una prueba de cumplimiento determina si los controles están siendo aplicados de manera que "CUMPLA CON" las políticas y procedimientos de la administración.

Una prueba sustantiva establece la suficiencia de los controles existentes en proteger a la organización de actividades fraudulentas. Es decir se verifica la totalidad, veracidad y exactitud de la información.

5.2.3 Reglas de Evidencia

La evidencia es cualquier información usada por el auditor 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 entrevistas, material extraído de la documentación correspondiente o interna, o de resultados de procedimientos de prueba de auditoría. Mientras toda la evidencia ayudará al auditor 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.

- Capacidades de la persona que proporciona la información o evidencia

  Ya sea dentro o fuera de la organización, el auditor siempre considera las capacidades de las personas que proporcionan la información, esto es también aplicable para el auditor.

- Objetividad de la evidencia

  La evidencia objetiva es mucho mejor que la evidencia subjetiva que requiere una interpretación o juicio considerable.

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

5.3 Obtención, Evaluación de Evidencia y Generación del Reporte de Auditoría

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

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.

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 por la organización. Sin embargo, el auditor habilidoso debe entender los componentes básicos de un reporte de auditoría y como comunicar adecuadamente los hallazgos de auditoría a la administración.

6 CODIGO DE ETICA PROFESIONAL

La Fundación de Auditores al Proceso Electrónico de Datos (EDPAF), expresó un código de Etica Profesional que guía la conducta personal y profesional de los auditores en proceso electrónico de datos.

Los auditores EDP deberán:

- Apoyar el establecimiento y cumplimiento de las normas, procedimientos y controles para sistemas de información.

- Cumplir con las Normas de Auditoría de Sistemas de Información adoptados por la fundación de auditores EDP (EDPAF).

- Servir en el interés de sus empleadores, accionistas, clientes y al público en general de una manera diligente, leal y honesta, adicionalmente no se deberá tomar partido en cualquier actividad ilegal o impropia.

- Mantener la confidencialidad de la información obtenida en el curso de sus actividades. La información no deberá ser usada para beneficio personal o divulgada a terceros no autorizados.

- Desarrollar sus actividades de una manera independiente y objetiva, además de evitar actividades que afecten, o puedan afectar, su independencia.

- Mantener un nivel de competitividad en los campos relacionados con auditoría y sistemas de información, a través de participaciones en actividades de desarrollo profesional.

- Ejerecer sumo cuidado al obtener y documentar material suficiente sobre el cual se basa sus conclusiones y recomendaciones.

- Informar la razonabilidad de los resultados del trabajo de auditoría llevado a cabo.

- Fortalecer el conocimiento de la dirección, clientes y el público en general para lograr su entendimiento en auditoría y sistemas de información.

- Mantener altos estándares de conducta y carácter en actividades personales y profesionales.

7 NORMAS GENERALES PARA LA AUDITORIA DE SISTEMAS DE INFORMACION

De igual manera la EDPAF (Fundación de Auditores al Proceso Electrónico de Datos) emitió normas generales para dirigir la práctica de auditoría a sistemas de información, estas son:

1 ACTITUD Y APARIENCIA .- En todos los asuntos relacionados a la auditoría, el auditor en sistemas de información debe ser independiente al auditado en actitud y aparencia.

2. RELACION ORGANIZACIONAL .- La función de auditoría en sistemas de información debe ser suficientemente independiente del área que está siendo auditada para permitir la realización objetiva de la auditoría.

3. CODIGO DE ETICA PROFESIONAL .- El auditor en sistemas de información debe cumplir con el código de ética profesional de la función de auditores EDP.

4. HABILIDAD Y CONOCIMIENTOS .- El auditor debe ser técnicamente competente, poseer las habilidades y conocimientos necesarios en la realización del trabajo de auditoría.

5. EDUCACION PROFESIONAL CONTINUA .- El auditor debe mantener la competencia técnica a través de la educación continua apropiada.

6. PLANEACION Y SUPERVISION .- Las auditorías de sistemas de información deben ser planeadas y supervisadas para proporcionar la certeza de que los objetivos de auditoría son logrados y la adhesión a estas normas es cumplida.

7. REQUERIMIENTO DE EVIDENCIA .- Durante el curso de la auditoría, el auditor en sistemas de información obtiene evidencia de naturaleza y suficiencia para apoyar los hallazgos y conclusiones reportados.

8. DEBIDO CUIDADO PROFESIONAL .- El debido cuidado profesional debe ser ejercido en todos los aspectos del trabajo del auditor en sistemas de información, incluyendo el cumplimiento de las normas de auditoría aplicables.

9. INFORME DEL ALCANCE DE LA AUDITORIA .- En la preparación de reportes, el auditor debe establecer los objetivos de la auditoría, el período cubierto, la naturaleza y el alcance del trabajo de auditoría realizado.

10. REPORTE DE HALLAZGOS Y CONCLUSIONES .- En la preparación de reportes, el auditor de sistemas de información debe revelar todos los hallazgos y conclusiones concernientes al trabajo de auditoría realizado y cualquier reserva o conclusión que el auditor tiene con respecto a la auditoría.

CAPITULO II

CONTROLES Y RIESGOS EN UN AMBIENTE DE SISTEMAS AUTOMATIZADO

II. CONTROLES Y RIESGOS EN UN AMBIENTE DE SISTEMAS AUTOMATIZADO

OBJETIVO

El auditor obtendrá los elementos para analizar los riesgos existentes en un ambiente de sistemas automatizado, así como los posibles controles a implantar para minimizar los riesgos identificados.

INTRODUCCION

EL principal objetivo de establecer controles sobre los sistemas automatizados es disminuir:

Los Riesgos de Aplicación:

- Acceso a las funciones de procesamiento de las transacciones o registros de datos resultantes.
- Datos ingresados para su procesamiento.
- Datos rechazados y partidas en suspenso.
- Procesamiento y registro de transacciones.

Los Riesgos del Departamento PEI:

- La estructura de organización y los procedimientos operativos del departamento PEI (Proceso Electrónico de Información) no garantizan un ambiente de procesamiento de datos que conduzca a la preparación de información.
- Los programadores pueden realizar cambios no autorizados en el software de aplicación, lo cual reducirá la confiabilidad de la información procesada en el sistema.
- Personas no autorizadas (empleados o terceros) pueden tener acceso directo a los archivos de datos a programas de aplicación utilizados para procesar transacciones, permitiéndoles realizar cambios no autorizados a los datos o programas.

1 RIESGOS DE APLICACION

Al considerar las implicaciones de auditoría de las posibles debilidades de la organización, debe tenerse en cuenta la importancia de las características del sistema.

Si la organización no posee controles de procesamiento computarizados para lograr los objetivos de una característica del sistema, se supone que existe una debilidad. Como las características del sistema abarcan los cuatro riesgos de auditoría PEI a nivel de aplicación y otros aspectos esenciales del procesamiento, es importante considerar de qué manera la organización alcanza los objetivos de control de procesamiento o funciones de procesamiento automatizado. A menudo, esto requiere confianza en los controles generales y controles independientes. Si no existen controles mitigantes, es posible que debamos reevaluar el alcance de los procedimientos sustantivos planeados.

1.1 Acceso a las Funciones de Procesamiento de las Transacciones a Registros de Datos Resultantes.

1.1.1 Riesgo

Personas no autorizadas pueden tener acceso a las funciones de procesamiento de transacciones de los programas de aplicación o registros de datos resultantes, permitiéndoles leer, modificar, agregar o eliminar información de los archivos de datos o ingresar sin autorización transacciones para su procesamiento.

1.1.2 Controles de Acceso

Los recientes avances en la tecnología para el Procesamiento Electrónico de Información (PEI) han ampliado el acceso a los sistemas automatizados y, por consiguiente, a la información almacenada en los archivos del computador. Con mayor frecuencia se permite el acceso, lectura y uso de datos automatizados a los departamentos usuarios.

Pero una vez que se otorga el acceso a los sistemas automatizados aumenta el riesgo de acceso no

autorizado, por ejemplo que los usuarios que solamente tengan autorización de lectura puedan:

- Ingresar transacciones
- Modificar transacciones
- Eliminar datos
- Recuperar datos
- Modificar archivos maestros (datos permanentes)

En esta situación y dependiendo de la naturaleza de las funciones de procesamiento que puedan realizarse con el software al que se accesa, un solo individuo podría llegar a realizar tareas incompatibles. Es muy raro que una organización otorgue a un mismo empleado tan amplio acceso. Existen tres etapas dentro del control de acceso: identificación, autentificación y autorización. Las funciones de identificación y autentificación, es decir, identificar al usuario y probar quien dice ser, son realizadas independientemente del acceso a las funciones y datos de procesamiento, no obstante, en el proceso de identificación, el usuario ingresa un código único al sistema que se utiliza como clave para determinar a qué funciones o datos de procesamiento puede accesar y, a menudo, las opciones con que contará una vez que haya accesado a los datos.

La autorización de acceso a las funciones y datos de procesamiento es logrado a través de rutinas que pueden ser incorporadas al software de sistemas o de aplicaciones, o ambos.

1.1.3 Análisis de controles

Menús

Un menú es un listado de funciones expuesto en la pantalla de una terminal para dirigir al usuario a las funciones apropiadas, muchos de los diseñadores de sistemas de aplicación utilizan menús para estructurar el acceso a dichos sistemas y guiar a los usuarios a través de niveles sucesivamente más detallados de ejecución y toma de decisiones. De la

misma manera los menús pueden ser armados para implantar la segregación de funciones.

Normas/perfiles de acceso

El software de control de acceso, los monitores de teleprocesamiento, el software de control de comunicaciones y otro software, incluyen tablas o bases de datos que asocian a los individuos y/o grupos con los recursos que se les permite usar. Además, pueden definir a que grupo pertenece un individuo y lo que se le permite hacer con un recurso determinado.

Acceso a los datos por programa

Los programas están limitados con respecto a los datos a los que pueden accesar y/o actualizar, y los individuos estan limitados con respecto a los programas que pueden utilizar.

Acceso a los datos y programas por dispositivos

De la misma manera en que se limita a los inividuos a ciertas funciones o que sólo se les permite el acceso a determinados datos, las restricciones de acceso pueden ser aplicadas a los dispositivos, usualmente terminales. Con frecuencia, el principal motivo del control de acceso es limitar el acceso de los individuos a las funciones y recursos autorizados. En algunos casos, particularmente cuando se procesa una aplicación "sensitiva" en un área físicamente protegida, dicha aplicación y sus datos estarán limitados a las terminales del área correspondiente. Esto puede constituir un nivel de control adicional además de las restricciones al acceso del personal a dichas transferencias.

Dispositivos de seguridad de terminales

Algunas organizaciones deciden implantar controles adicionales a los proporcionados por los monitores de teleprocesamiento, software de seguridad, software de control de comunicaciones o DBMS. Para ello, se equipa a las terminales con dispositivos de hardware y/o software especializados.

1.2 Datos Ingresados para su Procesamiento

1.2.1 Riesgo

Los datos permanentes y de transacciones ingresados para su procesamiento pueden ser impresos, incompletos o ser ingresados más de una vez.

1.2.2 Análisis de los controles

Controles de edición y validación

Los controles de edición y validación están diseñados para permitir la identificación de errores en los datos ingresados, ingresos duplicados, o datos que no satisfacen ciertos criterios preestablecidos de aceptación.

Los controles de edición y validación pueden contribuir significativamente a la exactitud del ingreso de datos, sin embargo, probablemente no sean los únicos controles en los cuales decidimos confiar. También deberíamos considerar otros controles de procesamiento y funciones de procesamiento automatizadas que contribuyan a la exactitud de los datos.

Verificación de ingreso por teclado

La verificación de ingreso por teclado puede ser utilizada como control de la exactitud de los datos ingresados. Con este proceso, los datos críticos seleccionados son reingresados identificando las diferencias entre el primer y segundo ingreso de datos. Luego, se investigan las diferencias y se corrigen las transacciones. Este tipo de verificación resulta útil para controlar la exactitud del ingreso de datos en sistemas no interactivos, ya que en este tipo de sistemas no se realizan controles de edición y validación hasta un punto posterior del procesamiento.

1.3 Datos Rechazados y Partidas en Suspenso

1.3.1 Riesgo

Los datos rechazados y las partidas en suspenso pueden no ser identificadas, analizadas y corregidas.

1.3.2 Análisis de los controles

Una transacción puede no pasar un control de edición si, por ejemplo, falta el número de cuenta o si el dígito verificador del número de cuenta es incorrecto.

Dependiendo del diseño del sistema de computación, los datos inválidos o no comparados pueden ser:

- Aceptados por el sistema e incluidos en un informe de excepciones.
- Incluidos en un archivo de partidas en suspenso dentro del sistema.
- Completamente rechazados.

Por lo general cuando los datos son rechazados el computador no retiene ningún registro de las partidas y, en consecuencia, los mismos deben ser controlados manualmente. Normalmente, el usuario es reponsable de asegurar que estas transacciones sean posteriormente corregidas.

Las partidas en suspenso pueden ser mantenidas en un sistema automatizado en una o más de las siguientes formas:

- En archivos separados físicamente.
- En registros separados dentro dos archivos maestros.
- Con los restantes registros de los archivos maestros pero identificados como un tipo de transacción separada por medio de indicadores.

Generalmente, el riesgo asociado con la corrección de transacciones inválidas o no comparadas es menor cuando se utiliza un archivo en suspenso que cuando las transacciones erróneas son aceptadas e incluidas en informes de excepción para su posterior corrección.

1.4 Procesamiento y Registro de Transacciones

1.4.1 Riesgo

Las transacciones reales que han sido ingresadas para su procesamiento o generadas por el sistema pueden perderse o ser procesadas o registradas en forma incompleta.

1.4.2 Análisis de los controles

Documentos fuente prenumerados

Al igual que en los sistemas de procesamiento manual el uso de documentos fuente prenumerados nos permite asegurar que las transacciones no se pierdan durante el procesamiento. El software de aplicación puede ser programado para asignar números de referencia secuenciales, controlar los números de referencia de las transacciones ingresadas para procesamiento o transacciones generadas por el sistema y/o para producir informes de excepción de documentos faltantes para su seguimiento.

Controles de sesión

Los controles de sesión son efectuados por el software de aplicación y están diseñados para emular un procedimiento de control de procesamiento por lotes.

Controles por lotes

Los controles por lotes se basan en la preparación de totales de control de los campos críticos antes del procesamiento. Estos totales de control son

comparados posteriormente con los totales generados por el computador.

Controles de balanceo programados

Los controles de balanceo programados son incorporados al software de aplicación para asegurar la exactitud e integridad de la actualización de datos.

Controles de etiquetas internas de archivos

Estos controles son ejecutados automáticamente por el software de administración de operaciones y/o software de administración de archivos de datos y pueden ser utilizados para asegurar que se utilizan las versiones correctas de los archivos de datos y programas de producción.

Controles de transmisión de datos

Los dispositivos estándar del software de transmisión de datos producen un cálculo de "prueba" con la información incluida en la transmisión. El resultado de dicho algoritmo es registrado en un mensaje de encabezamiento previo a la transmisión.

Procesamiento de reenganche y recuperación

Una interrupción del procesamiento puede originar la pérdida de las transacciones que se están procesando en ese momento, lo cual resulta especialmente grave cuando los datos son ingresados en forma interactiva y en los sistemas que utilizan un procesamiento de actualización inmediato. En estas situaciones, no se dispondrá de documentos impresos de respaldo y la posibilidad de determinar si una transacción fué completamente procesada antes de la interrupción quedará anulada.

Controles de corte programados

Los controles para prevenir un corte incorrecto pueden ser muy variados y generalmente, son

comparables a controles similares en un ambiente de procesamiento manual.

Los controles de procesamiento tratados en relación con este riesgo son particularmente importantes en sistemas en los que:

- Los datos ingresados o generados automáticamente actualizan los archivos de datos utilizados en más de una aplicación. Generalmente, estos sistemas son llamados sistemas integrados.
- Los programas generan automáticamente transacciones.

2 RIESGOS DEL DEPARTAMENTO PEI

2.1 Estructura Organizativa y Procedimientos de Operación PEI

2.1.1 Riesgo

La estructura de organización y los procedimientos operativos del departamento PEI no garantizan un ambiente de procesamiento de datos que conduzcan a la preparación de información.

La segregación de tareas en un departamento PEI centralizado típico, debe separar la responsabilidad relativa a cada una de las siguientes funciones:

- Administración
- Análisis de sistemas, diseño y programación de aplicaciones
- Mantenimiento del software de sistemas
- Operaciones
- Control de datos
- Seguridad de datos

Además, en los casos que corresponda, las siguientes funciones también deben ser segregadas: administración de base de datos, comunicaciones y coordinación de microcomputadoras.

Es posible que a medida que aumente la sofisticación y complejidad de los sistemas de información de una organización, se emplee personal mejor capacitado y se asignen al personal funciones de una mayor especialización. Debemos evaluar las funciones que puede llevar a cabo la gerencia del departamento PEI, los programadores de sistemas, los programadores de aplicaciones y los operadores.

Sistemas Computarizados Pequeños

En los sistemas automatizados pequeños, los usuarios pueden efectuar funciones que tradicionalmente tiene a su cargo el personal del departamento PEI. La gerencia debe tratar de compensar la falta de segregación de funciones implantando controles compensatorios.

2.1.2 Análisis de los controles

Manuales de operación y controles operativos diarios

Se deberá contar con manuales de operación a fin de que los empleados estén adecuadamente informados acerca de los procedimientos operativos vigentes.

La existencia de controles operativos diarios efectivos permite asegurar que el computador no sea utilizado sin autorización, que los archivos procesados sean los correctos y que no surjan errores o irregularidades de las operaciones del computador.

Los manuales de operación pueden ser examinados para determinar que incluyan procedimientos escritos claramente definidos para todas las actividades, procedimientos de reenganche y recuperación, etc.

Las posibles pruebas de los controles operativos diarios incluyen:

- Examinar los informes del sistema de registro de trabajos o los registros impresos de la consola y verificar:

  . La secuencia para comprobar que haya explicación de todo el tiempo de uso del computador.

  . Que exista evidencia de su aprobación por la gerencia.

  . Que se hayan tomado acciones apropiadas.

- Establecer si la gerencia ha recibido y aprobado un resumen del uso del computador.

Control sobre software sensitivo

El software de sistemas controla el funcionamiento de un computador. Aunque no procesa los datos, puede controlar el acceso a estos datos y su utilización. Por consiguiente, permite la posibilidad de que los programas y controles de aplicación sean burlados.

Existen diversos tipos de software de sistemas que pueden ser considerados "sensitivos". Los sistemas operativos incluyen funciones que pueden ser utilizadas para saltar o vulnerar los controles de acceso. Los monitores del sistema pueden modificar datos que ya han sido almacenados en la memoria del computador. El software de control de comunicaciones puede permitir el acceso a aplicaciones protegidas, los utilitarios y editores en línea (on line) pueden facilitar cambios a los programas o a la información almacenada, o permitir el acceso a los datos sin dejar rastro de los accesos o modificaciones.

Algunos utilitarios, tales como ZAP o DFU, están diseñados para facilitar "arreglos rápidos" del software de sistemas, programas objeto y archivos de datos, evitando de esta forma inconvenientes o demoras en el procesamiento. De igual forma, los editores en línea (on-line) son herramientas de productividad para la programación que permiten acelerar el proceso de desarrollo, prueba, revisión y corrección de fallas (debugging) de los programas. Debido a sus poderosas capacidades, y también a los conocimientos técnicos de los programadores de sistemas que suelen emplear estos productos sensitivos, su disponibilidad puede posibilitar

circunstancias en las que una persona pueda causar y ocultar errores o irregularidades.

Se pueden realizar las siguientes pruebas de los controles sobre software sensitivos.

- Obtener un listado de todo el software sensitivo.
- Obtener comprensión de los controles que aseguran que todo el software instalado esté autorizado y registrado.
- Partiendo de los directorios de las bibiliotecas, seleccionar una muestra de módulos de software de sistemas y verificar la autorización de la gerencia PEI para su incorporación.
- Determinar y confirmar si la gerencia supervisa el uso de este software y que quede constancia de dicha supervisión.
- En aquellos casos en que las utilerías son mantenidas por separado, probar las autorizaciones para su reinstalación y uso, y confirmar que los programas sean inmediatamente "borrados" al concluirse la tarea autorizada.

Controles sobre el desarrollo de sistemas

Los procedimientos para desarrollo, prueba e implantación de sistemas deben ser realizados en conformidad con las normas adoptadas por el departamento PEI.

El interés de mantener controles sobre el desarrollo de sistemas es porque permite determinar que los sistemas que procesan la información signficativa incluyen, una vez implantados, controles adecuados que operan de la manera esperada.

Como nos ocupamos principalmente de los sistemas de producción (es decir, sistemas utilizados para procesamiento de operaciones diarias), no es conveniente que, para obtener evidencia de auditoría, decidamos probar los procedimientos de desarrollo de sistemas. No obstante, si decidimos que los controles sobre el desarrollo de sistemas constituyen controles clave o si decidimos probar los procedimientos

relacionados respondiendo a expectativas del cliente, existen diversas pruebas que podemos realizar, Por ejemplo:

- Revisar las especificaciones escritas referentes a las nuevas aplicaciones.
- Determinar si las especificaciones para nuevas aplicaciones y las modificaciones de las aplicaciones existentes fueron preparadas de acuerdo con las normas de instalación.
- Determinar a través de conversaciones con los usuarios y el personal del departamento PEI, si el alcance de las modificaciones realizadas en las aplicaciones fueron significativas y si la participación del usuario fué la necesaria en el desarrollo de sistemas.

2.2 Procedimientos para Cambios a Programas

Los cambios a los programas o actividades de mantenimiento incluyen las tareas necesarias para que el software continue siendo operativo y adaptarlo a los cambiantes requerimientos de los usuarios. Se ha estimado que en la mayoría de las organizaciones más del 50% del tiempo de programación se emplea en modificaciones a los programas. Generalmente las modificaciones se realizan por las siguientes razones:

- Para corregir errores del software.
- Para adaptar el software en respuesta a cambios del hardware y/o software.
- Para modificar el software a fin de obtener mayor efectividad y eficiencia.

2.2.1 Medios de control

La evaluación de los controles de cambios a los programas es un complemento de nuestra evaluación de la segregación de funciones. Dada la capacidad técnica de los programadores, un inadecuado control de sus actividades podría tener efectos negativos sobre la capacidad de la organización para salvaguardar sus activos y procesar información en forma confiable.

La eficacia de los controles sobre cambios a los programas probablemente sea desde nuestra perspectiva, el aspecto más importante de los controles del departamento PEI. En ausencia de controles adecuados, no existirá forma de asegurar que los controles y las funciones de procesamiento automatizado son efectivas y han funcionado durante el período examinado.

El proceso para modificar sustancialmente el software generalmente debe ser el mismo que el utilizado en el desarrollo de nuevos sistemas. El proceso para otro tipo de modificaciones normalmente debe incluir lo siguiente:

- Los cambios sólo deben ser introducidos en las versiones de prueba del software y no en las versiones de producción.

- Los cambios sólo deben ser realizados por el personal de sistemas o programación.

- Los cambios deben ser respaldados por documentos. La documentación juega un papel importante en el mantenimiento del software. Facilitar las tareas del programador que se encarga de modificar el programa proporcionándole:

  . Una descripción general de lo que el programa hace.

  . Una descripción detallada de la forma de operación del programa (especificaciones del programa).

. Una descripción detallada de los datos ingresados al programa (input) y los resultados (informes y salidas de datos) producidos por el sistema (output).

- Todos los cambios deben ser revisados y aprobados por un individuo independiente de los programadores que realizaron las modificaciones al software.

- Es necesario llevar un registro permanente de todas las modificaciones.

- El gerente a cargo del desarrollo y programación de aplicaciones debe asegurarse de que los cambios de código hayan sido revisados y aprobados y además debe aprobar los resultados de las pruebas conjuntamente con la gerencia del departamento usuario. La aprobación debe ser previa a la transferencia del software modificado a la biblioteca de producción.

2.2.2 Análisis de los controles

La alteración del código fuente de un programa (escrita en un lenguaje de programación, por ejemplo COBOL) no afecta necesariamente el procesamiento de información. Esto se debe a que los cambios a los programas deben ser introducidos en una copia del código fuente del programa en una biblioteca de prueba y no en una biblioteca de producción.

Se pueden crear bibliotecas de prueba y de producción separadas físicamente o utilizar dispositivos indicadores de estatus del software de administración de bibliotecas. El acceso a las bibliotecas puede ser restringido por medio de un software de control de acceso. No obstante, se deberá tener en cuenta que, por lo general, este software no puede restringir el acceso a una persona autorizada a determinados programas si no se dispone de interfases especiales con otro software.

Con restricciones apropiadas, las bibliotecas de prueba pueden ser usadas por los programadores para realizar cambios a los programas y probar dichos cambios mediante la utilización de datos de prueba. Para que el procesamiento de datos reales se vea afectado, el programa en código fuente debe primero

ser compilado, editado en cadena y reingresado a la biblioteca de producción.

Desde la perspectiva de control, es esencial que los cambios a los programas sean aprobados por el usuario y el supervisor del programador antes de que el programa fuente modificado sea compilado y reingresado a la biblioteca de producción. Una vez que un programa modificado ha sido ingresado a la biblioteca de producción, cualquier cambio introducido en el mismo afectará el procesamiento en vivo. Para facilitar la supervisión de los cambios a las versiones en código fuente de los programas, se puede utilizar un software de administración de bibliotecas. Como alternativa, puede utilizarse un software de comparación de código fuente para hacer una comparación línea por línea del código fuente original y del modificado e identificar cada cambio. Es preferible que alguna de estas herramientas sea utilizada por el supervisor del programador como parte del proceso de revisión y aprobación. De lo contrario, su revisión de los cambios introducidos podría no ser efectiva.

Sistemas computarizados pequeños

No se puede generalizar con respecto a la efectividad de los procedimientos de cambios a los programas en los sistemas automatizados pequeños. En algunos casos, pueden ser tan eficientes o aún mejores que los de sistemas de mayor magnitud. En otros, pueden no ser satisfactorios.

Un factor importante en la evaluación de los riesgos y controles es determinar si el usuario tiene la posibilidad de modificar el software. En algunos sistemas de mini y microcomputadores, el usuario no tiene intervención directa en la preparación o mantenimiento del software dado que los paquetes de aplicación son comprados a proveedores externos. Habitualmente, y como parte del acuerdo de compra, el mantenimiento corre por cuenta del proveedor. En estos casos, el usuario no estará en condiciones de introducir cambios al software, particularmente cuando no se proporciona a los usuarios el código fuente de los programas; por consiguiente, el riesgo de cambios no autorizados no es significativo. Sin embargo, debemos asegurarnos de que los cambios efectuados por el proveedor del software sean adecuadamente probados por el cliente.

CAPITULO III

PLANEACION DE LA AUDITORIA EN INFORMATICA

III. PLANEACION DE LA AUDITORIA EN SISTEMAS

OBJETIVO

- Tomar decisiones de planeación sobre las partes o unidades del negocio.
- Identificar componentes.
- Establecer el enfoque de auditoría esperado.
- Obtener una comprensión global de las actividades del negocio.
- Desarrollar y documentar la comprensión de los sistemas relacionados con cada actividad del negocio.
- Presupuesto del tiempo en que se llevara a cabo la revisión y número de personas que participarán.

INTRODUCCION

Para realizar una adecuada planeación de la Auditoría en Informática, es necesario cubrir ciertos puntos de interés que nos permitirán determinar el tamaño y características del área dentro de la compañía a auditar, la complejidad de sus sistemas, organización y equipo; con lo cual podremos definir los alcances de la auditoría, las herramientas necesarias, el tiempo y el costo de la realización de la auditoría, a esto lo conoceremos como planeación.

Para lograr una buena planeación, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar, para lo cual es necesario realizar una investigación preliminar y algunas entrevistas previas y con base en esto realizar el programa de trabajo.

El proceso de planeación lo consideraremos en tres fases que se indican a continuación:

Planeación Estratégica.- Durante la planeación estratégica debemos incluir:

- Consideración del ambiente de control.
- Consideración del ambiente de sistemas de información.
- Una clara comprensión de los controles que utiliza la gerencia para supervisar las operaciones de la empresa.

Planeación Detallada.- En esta etapa debemos incluir:

- Una clara comprensión del flujo de transacciones en cada aplicación significativa.
- Una evaluación de la confiabilidad del sistema de control y del riesgo, estableciendo las áreas en que podemos confiar en los controles como fuente de satisfacción de auditoría y aquellas en las que no podemos confiar.

Planeación de los recursos de auditoría.- En este estado se determina el personal y las tareas de auditoría a desarrollar.

1 INVESTIGACION PRELIMINAR (PLANEACION ESTRATEGICA)

Es necesario iniciar el trabajo de obtención de datos con un contacto preliminar que permita concebir una idea global del ambiente de sistemas dentro de la compañía. Debemos comenzar con una visita al organismo, al área de informática y a los equipos de cómputo. Se debe realizar la investigación preliminar solicitando y revisando dos aspectos que pueden ser significativamente afectados por la utilización de sistemas computarizados por parte de la compañía:

- Ambiente de sistemas de información.
- Ambiente de control.

1.1 Ambiente de Sistemas de Información

Una parte integrada de la planeación estratégica consiste en el conocimiento del ambiente del sistema de información de la compañía. Aunque no es necesario que la información obtenida durante la planeación estratégica sea sumamente detallada, debe ser suficiente para permitirnos determinar, en términos generales, hasta que punto se ha automatizado el procesamiento de transacciones y la información relacionada, la complejidad de los sistemas y el grado en que las operaciones de la compañía dependen de los sistemas automatizados. Esta información puede afectar nuestras evaluaciones del riesgo inherente y de control, la naturaleza y nivel de los conocimientos sobre computación requeridos para la planeación y ejecución de la auditoría en relación con los sistemas automatizados y las expectativas de la empresa; entre los puntos a considerar se incluyen:

- Estructura Organizativa de las operaciones PEI (Proceso Electrónico de Información).
- Naturaleza de la configuración de equipos
- Naturaleza y alcance del procesamiento automatizado de la información para las principales áreas o tipos de transacciones.

1.1.1 Estructura organizativa de la operaciones PEI

La obtención de una comprensión general de los sistemas de información debe comenzar con la estructura organizativa y administración de la misma. Esta comprensión permite al equipo de trabajo analizar el ambiente de control. La comprensión de la estructura organizativa y gerencial del departamento PEI proporciona generalmente las bases para establecer una relación de trabajo efectiva con el personal responsable de los sistemas automatizados.

Esta información debe incluir:

- Identificación del responsable del departamento PEI
- De quién depende dicho puesto
- Si existe un comité de dirección PEI
- Si el grupo PEI está organizado en forma centralizada o descentralizada entre varias unidades operativas.

Organización interna

La magnitud de la empresa puede tener poca influencia sobre el tipo o complejidad de sus sistemas de computación. Por ejemplo, según la naturaleza del negocio, una pequeña empresa puede contar con un importante y complejo sistema distribuido en tanto que una empresa más grande puede tener un sistema centralizado más pequeño. Por estas y otras razones, no se puede presentar un plan de organización que se adapte a todas las empresas.

Las organizaciones que cuentan con sistemas más grandes o más sofisticados generalmente tienen mayor cantidad de niveles gerenciales y de supervisión, como así también mayor especialización en las funciones de programación, análisis y operaciones. Por el contrario, las organizaciones cuyos departamentos PEI son más pequeños o menos sofisticados generalmente incluyen menor cantidad de niveles con menor especialización en cada una de las funciones. En un ambiente descentralizado algunas de las funciones pueden ser realizadas en el departamento usuario.

Gerencia

La responsabilidad general por la planeación, organización, dirección y control de las actividades de procesamiento de datos recae en un individuo o en un comité de sistemas. Tradicionalmente, los computadores han sido usados con mayor frecuencia para procesar datos contables y financieros. Por ello, el individuo responsable de las actividades de procesamiento dependía habitualmente del principal funcionario administrativo-financiero. Un enfoque más reciente considera que la información es un recurso de toda la organización y que los sistemas pueden procesar cualquier tipo de información gerencial. A raíz de este nuevo concepto, los sistemas automatizados han comenzado a salir del área de los gerentes administrativo-financieros para pasar a la de los profesionales en tecnología de sistemas de información que en muchos casos dependen directamente del principal funcionario operativo de la organización.

Organización de las actividades

Existen dos categorías funcionales básicas por debajo del nivel gerencial dentro de las cuales se clasifican las funciones del departamento PEI:

- Sistemas y programación

- Operación

La función de sistemas y programación consiste en el desarrollo de sistemas y modificaciones a los mismos y la función de operación incluye la responsabilidad por el procesamiento diario. La preocupación fundamental con respecto a la organización de un departamento PEI es que su personal no realice funciones incompatibles. Un punto importante para alcanzar este objetivo es que exista una clara división (segregación de funciones) entre estas dos áreas funcionales básicas. Al considerar la segregación de funciones, debemos concentrarnos en las responsabilidades funcionales más que en los títulos de los individuos que integran la estructura de la organización; el hecho de que el cliente no posea grupos de sistemas y programación y operación no significa necesariamente que estas funciones no estén adecuadamente segregadas.

Cambios que pueden afectar la estructura organizativa

Las estructuras organizativas de los departamentos PEI evolucionan continuamente en respuesta a los cambios tecnólogicos. Existen tres nuevos conceptos que probablemente tengan gran impacto en la organización y administración de sistemas computarizados:

- La creciente capacitación del usuario, unida a una tecnología cada vez más avanzada, crean un entorno de sistemas en el cual los usuarios participan más activa y directamente. Los días en que los usuarios se conformaban con enviar su requerimiento de nuevos informes y aguardaban durante meses su desarrollo ya han pasado.

- Los costos decrecientes del hardware y una capacidad cada vez mayor de los computadores pequeños han permitido que los microcomputadores proliferen dentro de las organizaciones. La conformación de redes con gran cantidad de unidades y el uso de aplicaciones independientes, incidirá en la estructura organizativa de la mayoría de los sistemas computarizados.

- Debido a la rápida y permanente evolución de la tecnología, los sistemas computarizados están en un estado de cambio contínuo. En la actualidad muchas organizaciones tienen un grupo de trabajo dedicado en forma exclusiva al desarrollo de nuevos sistemas o a efectuar cambios estructurales radicales a los ya existentes. La importancia de una adecuada supervisión y control de las modificaciones efectuadas a los sistemas de la organización debe ser recalcada en forma permanente.

1.1.2 Naturaleza de la configuración PEI

En la planeación estratégica, es necesario considerar los riesgos inherentes y de control asociados con los sistemas automatizados. Para ello, resultará conveniente obtener una visión general de la configuración PEI. Esta información también nos ayuda a considerar la magnitud y complejidad de los sistemas automatizados del cliente.

La estructura del sistema en uso puede tener implicaciones de auditoría significativas. Esto le permite al auditor lograr una comprensión de los sistemas de la organización y obtener evidencia de control en una sola unidad. En los sistemas descentralizados y de procesamiento distribuido de datos, cada computador tiene normalmente su propia organización de Proceso Electrónico de Información (PEI), programas de aplicación y software de sistemas. En consecuencia, será necesario visitar cada unidad que potencialmente posea significatividad de auditoría. Aunque las políticas de la empresa establezcan el uso de procedimientos idénticos en todas las unidades, debemos considerar si los procedimientos son aplicados en forma uniforme.

La visión general de la configuración puede incluir lo siguiente:

- Tipo, número y lugar de las principales unidades de procesamiento (CPU's).
- Si las CPU's están interconectadas.
- Si el procesamiento es centralizado o descentralizado.
- Si el ingreso de datos se efectúa únicamente en los lugares de procesamiento o en forma remota.
- Software de sistemas utilizado en las principales unidades de procesamiento que pueda proporcionar al personal PEI capacidad para leer, agregar, modificar o eliminar información almacenada en archivos de datos o bibliotecas de programas. Dicho software puede incluir:

  . Editores On-Line

  . Monitores de teleprocesamiento.

  . Utilerías con significatividad de auditoría y control.

  . Software de recuperación de datos.

  . Lenguajes de cuarta generación.

- Software utilizado para restringir el acceso a los programas y datos en las principales unidades de procesamiento PEI, tales como el software de control de acceso.

- Políticas de desarrollo y adquisición de software.

El alcance de la recopilación de información en la planeación estratégica varía según los trabajos. Por ejemplo, en el caso de clientes importantes con diversas unidades y sistemas descentralizados o distribuidos, resultará más difícil obtener la mayor parte de la información durante la planeación estratégica. En el caso de pequeños clientes con sistemas centralizados, la información puede ser obtenida con más facilidad. Debe destacarse que la información que no fué obtenida durante la planeación estratégica debe ser obtenida durante la planeación detallada si se deposita confianza en los controles de procesamiento y funciones de procesamiento computarizados.

1.1.3 Naturaleza y Alcance del Procesamiento Automatizado de la Información para las Principales Areas o Tipos de Transacciones

Como parte de nuestra comprensión de los sistemas automatizados de la organización, es necesario considerar en qué grado el cliente ha automatizado el procesamiento de transacciones. Esta información será útil para evaluar el riesgo inherente y de control e identificar la naturaleza de las aptitudes requeridas para la planeación y ejecución de la auditoría con respecto a los sistemas automatizados.

El nivel de detalle de la información a obtener en la planeación estratégica varía según factores tales como tamaño y complejidad de los sistemas automatizados de la organización. Entre los ejemplos del tipo de información que puede ser obtenida sobre los sistemas que respaldan los principales tipos de transacciones se incluyen:

- Objetivo del sistema

- Interfases dentro del sistema y con otros sistemas

- Volúmen aproximado de transacciones procesadas por el sistema

- Nombres de los paquetes de software comprados que se utilizan en el sistema
- Métodos de ingreso de datos (interactivo, no interactivo)
- Tiempos de entrega
- Usuarios que no utilizan la computadora
- Tipo de procesamiento (independiente o distribuido)
- Resultados recientes de los trabajos de auditoría relacionados con el sistema
- En caso de ser una auditoría recurrente (periódica) es necesario incluir las modificaciones significativas al sistema desde la última vez que se realizó una planeación

En un exámen recurrente, resulta coveniente que en la planeación estratégica nos concentremos en las modificaciones a los sistemas de la organización. Los nuevos sistemas y los cambios significativos a los existentes tienen, por lo general, impacto sobre nuestras evaluaciones del riesgo inherente y de control y las implicaciones de dichas modificaciones sobre nuestro enfoque de auditoría deben ser consideradas sin demora en el proceso de planeación.

1.2 Ambiente de Control

El ambiente de control es el conjunto de condiciones en el cual operan los sistemas de control. Al evaluar este ambiente, debemos tomar en cuenta el enfoque hacia el control por parte de la dirección y la gerencia general, la organización gerencial y el marco para ejercerlo. (El ambiente de control tiene gran influencia sobre nuestra posibilidad de confiar en los controles como fuente de satisfacción de auditoría).

La gerencia del departamento PEI, conjuntamente con la gerencia general, es la responsable de la planeación, organización, integración, dirección y control del departamento. Una buena gerencia brinda el beneficio de asegurar que el procesamiento de datos sea realizado en forma eficiente y que el departamento reciba los medios adecuados para

permitir el efectivo desempeño de sus responsabilidades.

Una función importante de la gerencia del departamento PEI es crear y mantener un adecuado ambiente de control. La calidad de la gerencia puede influir directamente sobre el ambiente de control y, por consiguiente, sobre la potencial confiabilidad de la información. Si los empleados perciben que la gerencia del departamento PEI no asume un compromiso con la noción de control, es probable que no le presten a estos temas la importancia adecuada. Por ejemplo debemos estar alertas a situaciones en las que la segregación de funciones parece apropiada, pero en las prácticas operativas poco estrictas permiten que los empleados no cumplan con los procedimientos prescritos.

Un fuerte ambiente de control nos permite depositar mayor confianza en los controles de la organización, seleccionar controles y funciones de procesamiento computarizado como fuentes de satisfacción de auditoría y posiblemente reducir la cantidad de evidencia requerida para lograr nuestro objetivo de auditoría. A continuación se incluyen algunos de los posibles temas relacionados con sistemas computarizados que deben ser considerados en la evaluación de la efectividad de un ambiente de control:

- El enfoque hacia el control por parte de la dirección y de la gerencia general

  . En que medida el estilo gerencial del departamento PEI se caracteriza por la planeación o improvisación.

  . Importancia que la gerencia del departamento PEI asigna a los controles; la celeridad y forma de reaccionar ante las recomendaciones de los auditores internos y externos.

  . Celeridad y efectividad de la respuesta de la gerencia del departamento PEI ante situaciones urgentes.

- Organización Gerencial

  . La posición del jefe del departamento PEI en la estructura organizativa de la empresa.

  . El nivel de rotación del personal del departamento PEI.

  . Si la delegación de responsabilidades y autoridad dentro del departamento PEI es adecuada, y en qué medida la autoridad y las responsabilidades delegadas han sido definidas y comprendidas.

  . Si la gerencia del departamento PEI participa en el concepto de segregación de funciones y si está en conocimiento de áreas en las que existe una concentración de funciones incompatibles.

  . El grado en que la gerencia de otros departamentos participa en las decisiones importantes de desarrollo de sistemas (posiblemente a través de un comité directivo o un grupo similar).

  . Si las actividades del departamento PEI son supervisadas por una función de auditoría interna independiente y competente.

- Marco para el control gerencial

  . Estadísticas clave y otra información utilizada para controlar el departamento PEI.

  . Si los planes y presupuestos financieros son utilizados para controlar los costos del departamento PEI.

  . Si se utilizan metodologías formales y efectivas de mantenimiento y desarrollo de sistemas de aplicación.

  . Métodos con los cuales se supervisa y aplica la segregación de funciones incompatibles.

  . Mecanismos por los cuales la gerencia del departamento PEI identifica y responde a situaciones inusuales o excepcionales.

2 EVALUACION DEL RIESGO INHERENTE Y DE CONTROL

La evaluación del riesgo es una parte integrante del desarrollo de un plan de auditoría. Las características específicas de los sistemas automatizados crean riesgos que, por lo general, son diferentes a los de un entorno de procesamiento manual. Si bien los objetivos de la gerencia con respecto a los sistemas de información y de control no se ven afectados por los medios utilizados para procesar los datos y son aplicables tanto a entornos manuales como computarizados, la forma de implantación de los controles diseñados para reducir al mínimo los riesgos propios de los sistemas computarizados pueden ser diferentes.

La información obtenida anteriormente en la planeación estratégica puede ser útil para considerar el riesgo inherente y de control. Entre los factores específicos de los sistemas de información computarizados a considerar, se incluyen:

- El grado de automatización del procesamiento de información para las principales áreas y tipos de transacciones.

- La complejidad relativa de los sistemas automatizados.

- La eficiencia de la estructura organizativa entre los sistemas computarizados de la empresa.

- El grado de dependencia hacia los sistemas automatizados.

- El uso de software de sistemas sensitivo que puede permitir a empleados expertos realizar cambios no autorizados a los datos y programas.

3 PLANEACION DETALLADA

Durante la planeación estratégica, la comprensión de un componente puede no ser suficiente para determinar el enfoque de auditoría esperado. Es posible que se

necesite información adicional para evaluar el riesgo e identificar los controles clave, incluyendo las funciones de procesamiento computarizadas en que podríamos confiar. Esta información es obtenida durante la Planeación Detallada. En esta etapa es cuando obtenemos y documentamos la comprensión de los aspectos relevantes de los sistemas de información del cliente y los controles generales relacionados.

Para facilitar la comprensión de los controles, estos han sido clasificados de la siguiente manera:

- Ambiente de control (véase planeación estratégica en páginas anteriores).

- Controles Directos: Son aquellos diseñados para evitar o detectar errores o irregularidades que afectarían a la información general y aquellas funciones de procesamiento computarizado que involucran el desarrollo de un aspecto escencial del procesamiento de transacciones e información directamente relacionada, desde su exposición hasta la información en reportes finales. Estos controles y funciones de procesamiento computarizado constituyen fuentes de satisfacción de auditoría. Los controles directos abarcan controles gerenciales e independientes, controles de procesamiento y funciones de procesamiento computarizadas.

- Controles Generales: Son aquellos que contribuyen significativamente a la efectividad de los controles directos. Abarcan la segregación de funciones incompatibles y controles del departamento PEI. Los controles generales no proporcionan satisfacción directa de auditoría. Al considerar la confianza en los controles directos como fuente de satisfacción de auditoría, debemos considerar si las deficiencias de los controles generales pueden afectar la efectividad de los controles directos.

3.1 Distinción entre controles directos y controles generales

La efectividad de los controles directos depende a menudo de los controles generales relacionados, por ejemplo, consideremos un sistema de cuentas por pagar

en el que los informes de recepción y las facturas del proveedor son relacionadas por el computador. Este proceso es un control directo que puede proporcionarnos evidencia, de que las compras representan mercancías recibidas. Si se pudieran efectuar cambios a los programas (considerado como un control general) puede disminuir nuestra posibilidad de confiar en los controles directos como fuente de satisfacción de auditoría. Los controles sobre cambios a los programas contribuyen a la efectividad de los controles directos pero no proporcionan por sí mismos satisfacción de auditoría.

Por consiguiente, raramente confiaremos en controles directos cuando se considera que los controles generales son débiles. Obtenemos evidencia sobre la operación de los controles generales solamente como una extensión de la obtención de evidencia respecto de la efectividad de los controles directos, incluyendo las funciones de procesamiento computarizadas. Sin embargo, es probable que deseemos considerar ciertos controles generales con mayor detalle respondiendo a expectativas de la empresa.

3.2 Distinción entre controles directos y funciones de procesamiento computarizadas

Las funciones de procesamiento computarizadas son pasos determinados en el sistema de la organización que se ocupan de las transacciones e información relacionada desde su origen hasta su inclusión en el documento que corresponda. Incluyen tareas tales como cálculo, registro, comparación y acumulación de datos generales. Los controles pueden ser acciones realizadas por la gerencia, un representante o un empleado de la organización o un software, o pueden incluir dispositivos para salvaguardar activos a fin de detectar errores o irregularidades.

La distinción entre funciones y controles de procesamiento no siempre son claras. Algunas funciones de procesamiento (por ejemplo: edición, validación o comparación) también representan controles ya que son diseñadas para evitar o detectar errores o irregularidades. Otras funciones de procesamiento (por ejemplo: registro, cálculo y acumulación) no constituyen controles en el sentido usual de la palabra ya que no están especialmente dirigidas a evitar o detectar errores o

irregularidades, pero que constituyen funciones significativas dentro del proceso automatizado.

Las funciones de procesamiento que representan controles como así también las que son aspectos esenciales del proceso automatizado pueden ser funciones significativas desde el punto de vista del auditor. Es decir, son funciones importantes con respecto a la exactitud e integridad de los datos de salida del sistema y por lo tanto, son funciones en las que el auditor debe concentrar su atención. Hay dos razones principales por las cuales son significativas. En primer lugar, pueden representar una fuente de satisfacción para el objetivo de auditoría. En segundo lugar, cuando no se puede lograr confianza, el auditor aún necesita obtener evidencia, en este caso evidencia sustantiva, de que los aspectos esenciales de la función de procesamiento han sido realizados satisfactoriamente para las transacciones procesadas.

3.3 Riesgos en la Auditoría

Un aspecto importante durante la planeación detallada es la consideración de los riesgos en la auditoría. Se han definido cuatro riesgos inherentes de aplicación y tres riesgos inherentes del departamento PEI.

Los cuatro riesgos que son considerados a través de la implantación de controles de aplicación son los siguientes:

- Acceso a las funciones de procesamiento de las transacciones o registros de datos resultantes
- Datos ingresados para su procesamiento
- Datos rechazados y partidas en suspenso
- Procesamiento y registro de transacciones

Los tres riesgos del departamento PEI son:

- Estructura Organizativa y procedimientos de operación PEI

- Procedimientos para cambios a los programas
- Acceso general a los datos o programas de aplicación

3.4 Comprensión de los Sistemas de Aplicación

3.4.1 Obtención de una comprensión global del sistema

La identificación de las actividades del negocio es el primer paso para dividir los sistemas de la organización en partes más manejables.

Esta comprensión puede ser documentada en un diagrama resumido, no debe ser muy detallado ya que dentro de la planeación obtendremos una visión general del sistema, la cual estará destinada a ayudar al equipo de trabajo a definir los límites del sistema e identificar puntos de transferencia importantes a y de otros sistemas.

Como parte del desarrollo de la visión general. Es conveniente considerar ciertos aspectos de la segregación de funciones. La segregación de funciones incompatibles puede ser considerada en dos niveles:

a) La segregación de funciones incompatibles entre las actividades del negocio.

b) La segregación de funciones específicas relacionadas con el procesamiento de transacciones y con el análisis de los resultados del procesamiento.

No debe asumirse automáticamente que una inadecuada segregación de funciones entre las actividades del negocio nos impedirá confiar en el sistema. La segregación de funciones incompatibles debe ser considerada en el contexto de los controles directos en que deseamos confiar.

3.4.2 Identificación de los controles gerenciales y controles independientes

Los controles gerenciales y los controles independientes son controles directos aplicados por

individuos que no participan en el procesamiento y son diseñados para detectar errores o irregularidades que puedan ocurrir antes o durante el procesamiento. Comprenden revisiones, análisis, comparaciones, conciliaciones, etc.

Los controles gerenciales y controles independientes, resultan a menudo fuentes efectivas y eficientes de satisfacción de auditoría. Es conveniente considerar estos controles en una primera etapa del análisis de los sistemas de información del cliente, porque normalmente afectan en forma integral un grupo de componentes o componente.

Nuestra comprensión de los controles gerenciales y controles independientes debe incluir una consideración del grado en que dichos controles dependen del procesamiento computarizado de transacciones e información directamente relacionada. Si un control gerencial o independiente depende del procesamiento computarizado, puede ser necesario obtener una comprensión de dicho procesamiento. Se requiere la aplicación de criterio para determinar el grado de comprensión del procesamiento computarizado relacionado con los controles.

3.4.3 Identificar específicamente las características del sistema que pueden proporcionar satisfacción de auditoría

La información recopilada no necesita ser extensa y debe incluir los aspectos automatizados y manuales del sistema. Puede resultar útil realizar un seguimiento de una selección de transacciones a través del sistema. Es necesario concentrarse en los procesamientos relacionados con los campos de datos con significatividad de auditoría potencial. Aunque probablemente esta información relevante pueda ser obtenida de los usuarios, es conveniente confirmar nuestra comprensión con el personal del departamento PEI responsable del sistema.

Al recopilar información sobre el sistema, debemos documentar aspectos tales como:

- Tipo de procesamiento (actualización inmediata o diferida).

- Utilización de software de administración de base de datos que puede permitir a otros usuarios de los sistemas de información de la organización, el acceso a los datos relacionados con este grupo de componentes.

- Métodos de ingreso de datos (interactivo, no interactivo o transacciones generadas por el sistema).

- Puntos del procesamiento en los que los usuarios tienen acceso a los datos.

- Puntos en los que se producen rechazos de datos y procedimientos seguidos para la identificación, seguimiento y reprocesamiento de los datos rechazados.

- El grado de participación del usuario y de auditoría interna en el control de la integridad del procesamiento.

- Puntos de transferencia hacia/desde otros sistemas (interfases).

- Mantenimiento de datos permanentes (archivos maestros).

- Pérdida del rastro de auditoría en salidas impresas.

- Modalidad de procesamiento (centralizado, descentralizado o distribuído).

Esta información proporcionará la base para la identificación de controles de procesamiento y funciones de procesamiento computarizadas específicas.

3.4.4 Identificar los controles de procesamiento (manuales o computarizados) y funciones de procesamiento computarizadas específicas que satisfacen los objetivos de las características del sistema

Antes de identificar los controles de procesamiento y funciones de procesamiento computarizadas, debe considerarse el nivel de capacidad técnica que podría requerirse.

Al revelar los controles de procesamiento y funciones de procesamiento computarizadas deberá consultarse tanto a los usuarios como al personal del departamento PEI dado que muchos sistemas de aplicación son diseñados para ser amigables para usuarios no experimetados, por lo que sus aspectos complejos son invisibles para dichos usuarios. Por consiguiente, los usuarios a menudo responden a las preguntas sobre el funcionamiento de un sistema desde su propia percepción y no con base a la comprensión de las funciones de procesamiento involucradas.

En ocasiones son varios los controles de procesamiento y funciones de procesamiento computarizadas que puedan satisfacer los objetivos de una determinada característica del sistema. Para mejorar la eficiencia, debemos documentar los controles y funciones que son considerados potencialmente clave.

3.4.5 Identificar los controles específicos que mitigan los riesgos del departamento PEI para cada uno de los controles directos potencialmente clave

Si un control directo es potencialmente clave e involucra procesamiento automatizado, debemos tener una clara comprensión del grado en el que indirectamente estamos depositando confianza en los controles del departamento PEI, y determinar el nivel de conocimientos técnicos requeridos para identificar y evaluar los riesgos y controles del departamento.

Los controles del departamento PEI son normalmente aplicables a todos los controles directos que operan en un mismo ambiente. Una clara identificación de los controles PEI existentes en cada organización promueve la eficiencia porque con frecuencia podemos considerar los riesgos del departamento una sola vez para todos los controles directos que operan en el mismo ambiente. Esto nos permite coordinar nuestra consideración de los controles del departamento PEI entre los componentes.

No debe asumirse automáticamente que los controles del departamento PEI son los mismos para todos los controles directos que operan en un mismo ambiente, ya que algunos de ellos pueden ser específicos para determinadas aplicaciones.

La información sobre los centros de procesamiento obtenida durante la planeación estratégica es útil como punto de partida para la identificación de los ambientes PEI. En algunos casos no será necesario obtener información adicional. En otros, se requerirán preguntas adicionales al personal del departamento PEI. Estas investigaciones deben ser muy específicas con respecto a los ambientes en los que operan los controles directos potencialmente clave.

El objetivo consiste en identificar los controles que mitigan los riesgos del departamento PEI en relación con los controles directos potencialmente clave. Los controles del departamento deben ser considerados en el contexto de los programas (software de aplicación y de sistemas) y archivos de datos relacionados con los controles directos.

Los procedimientos de investigación generalmente deben ser dirigidos al personal del departamento PEI. Debe tomarse la precaución de explicar el objetivo de las investigaciones y concentrar la discusión sobre la forma en que los riesgos del departamento son reducidos a un nivel aceptable en relación con los controles directos potencialmente clave.

3.4.6 Consideración de posibles debilidades

Las debilidades de los controles del departamento PEI deben ser documentadas juntamente con los controles directos potencialmente clave con los que estén relacionadas. Como los controles del departamento PEI no proporcionan por sí mismos evidencia directa de auditoría, el impacto de estas debilidades debe ser evaluado en términos de su efecto sobre los controles directos.

Las debilidades de los controles pueden, a menudo, ser mitigadas por controles específicos de una aplicación. Por ejemplo la organización podría no haber implantado software de control de acceso, por lo que podría concluirse que el riesgo de acceso general no autorizado no ha sido adecuadamente mitigado. No obstante, pueden existir controles de acceso dentro del propio sistema de aplicación en los que podríamos confiar para mitigar este riesgo.

El impacto de debilidades del departamento PEI puede ser atenuado en los sistemas pequeños de computación por las siguientes razones:

- En algunos sistemas pequeños de computación no existe un departamento PEI. Sin embargo, los procedimientos operativos de los departamentos usuarios y la segregación de funciones incompatibles pueden ser efectivas para producir un ambiente PEI que permita la preparación de información confiable.

- Los procedimientos para cambios a los programas pueden ser débiles. No obstante, si el cliente sólo utiliza paquetes de software comprados y no tiene acceso a código fuente, es posible que el riesgo de cambios no autorizados a los programas sea bajo.

- Pueden existir pocos controles sobre el acceso general, sin embargo, si no hay dispositivos de telecomunicaciones y si no hay acceso rutinario de terceros al sistema, es probable que el riesgo de acceso no autorizado sea bajo.

4 PLANEACION DE LOS RECURSOS DE AUDITORIA

Los auditores en sistemas de información son un recurso limitado en muchas organizaciones y su tiempo debe ser planeado y programado apropiadamente. El auditor 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 asignen al equipo tareas de auditoría específicas.

4.1 Recursos de Personal

Los directores de auditorías en sistemas de información deben tener un conocimiento de los recursos que están disponibles dentro de la organización para realizar auditorías. Los auditores pueden contar con diversos antecedentes, incluyendo programadores, auditores financieros, licenciados o ingenieros con diversos grados de experiencia, Auditores Certificados (CISA).

4.2 Restricciones en la Conducción de una Auditoría

Aunque una organización de auditoría puede estar dotada con personal que posea una mezcla apropiada de las habilidades requeridas, las restricciones pueden limitar la disponibilidad de su personal. Las restricciones normalmente incluyen las siguientes:

- Rotación de empleados recientes o no disponibilidad.
- Violación de fechas límite o fechas de procesamiento cíclicas.
- Falta global de conocimiento o documentación.

Para entender estas restricciones en la conducta de una auditoría dada, el auditor de sistemas debe tener una buena comprensión de las técnicas globales de administración del proyecto. Frecuentemente, estas restricciones pueden ser evitadas por una planeación adecuada.

4.3 Técnicas de Administración del Proyecto

Han sido desarrolladas numerosas técnicas de administración del proyecto que pueden ser compradas para administrar proyectos de auditoría. 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 un tiempo requerido para cada tarea de auditoría dando la debida consideración a la disponibilidad de los auditados.

- Reporte de la actividad del proyecto vs lo planeado

  Debe existir algún tipo de sistema que reporte el progreso actual de la auditoría comparado contra los pasos planeados.

- Ajustar el plan y tomar acciones correctivas cuando se requieran

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

4.4 Definir, Organizar y Monitorear Tareas de Auditoría

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

Las labores de administración de proyectos generalmente siguen las tareas de administración de proyectos discutidos brevemente en el punto 4.3.

4.5 Capacitación de Personal

La tecnología en los sistemas de información está cambiando constantemente. La capacitación debe mantener la competencia individual del auditor a través de las actualizaciones de las técnicas existentes, así como una capacitación dirigida hacia nuevas técnicas de auditoría y áreas tecnológicas.

CAPITULO IV

SEGURIDAD EN UN CENTRO DE COMPUTO

IV. SEGURIDAD EN UN CENTRO DE COMPUTO

OBJETIVO

Analizar y evaluar el sistema de control diseñado para salvaguardar la instalación de cómputo de amenazas de daños, errores o destrucción ya sea accidental, intencional o natural.

La forma de lograr este objetivo es mediante las pruebas y evaluación de:

- Controles de Acceso Físico.
- Controles de Acceso Lógico.
- Continuidad de Operaciones.

INTRODUCCION

Los controles de seguridad dentro de un centro de cómputo incluyen las siguientes áreas:

Controles de acceso físico.- Los cuales deben contemplar los medios físicos para salvaguardar el acceso y el medio ambiente de control.

Las funciones del auditor en esta área de seguridad son:

- Evaluar la seguridad física y el ambiente de control en el centro de cómputo y los medios para determinar la efectividad del mismo.

- Pruebas de control sobre las instalaciones de seguridad física para determinar su funcionamiento y efectividad mediante la aplicación de técnicas de auditoría.

- Evaluar el ambiente de seguridad física para determinar si los objetivos de control fueron logrados, a través del análisis de los resultados de prueba y otras evidencias de auditoría.

Controles de acceso lógico.- Dentro de los alcances de la salvaguarda de las instalaciones de cómputo están los controles de acceso lógico.

El objetivo del auditor en esta área de seguridad es analizar y evaluar las políticas, estructura organizacional, procedimientos operativos y controles de acceso usados para proteger el software de archivos de datos contra manipulación, destrucción y exposición no autorizados.

Las funciones del auditor en esta área son:

- Evaluar los controles sobre rutas de acceso potenciales dentro del sistema para asegurar su eficiencia y efectividad, revisando las apropiadas características de seguridad de hardware y software e identificando cualquier deficiencia o redundancia.

- Probar los controles sobre rutas de acceso para determinar su funcionamiento y efectividad mediante la aplicación de técnicas de auditoría.

- Evaluar el ambiente de control de acceso para determinar que los objetivos de control fueron logrados, a través de analizar los resultados de la prueba y otras evidencias de auditoría.

Continuidad de operaciones.- Consiste en la idea de que una compañía debe sobrevivir aún cuando ocurra un desastre. Sin embargo, muchos planes rigurosos y asignación de recursos son necesarios para adecuar el plan a tales eventos.

El objetivo en esta área es analizar y evaluar las políticas y procedimientos concernientes a planear contingencias para asegurar que la organización responda efectivamente a desastres y otras situaciones de emergencia.

1 COMPONENTES DE UNA BUENA POLITICA DE SEGURIDAD

Para que la seguridad sea satisfactoriamente implantada y mantenida, el alcance y propósito de la misma debe ser establecido y comunicado a todas las partes apropiadas. La forma de lograr este esfuerzo es el establecimiento formal de una política que sirva para mejorar el conocimiento de la seguridad dentro de la organización. Los componentes clave que debería incluir la política son los siguientes:

1.1 Compromisos y Apoyo de la Dirección

La dirección debe demostrar un compromiso con la seguridad. Esto puede ser mejor logrado a través de un conocimiento formal de la seguridad y que el entrenamiento sea claramente aprobado y soportado por la dirección, lo cual puede requerir un entrenamiento especial a nivel directivo ya que no necesariamente la dirección es experta.

1.2 Filosofía de Acceso

El acceso a la información computarizada debe estar basada en "la necesidad de conocer y la necesidad de hacer".

1.3 Autorización de Acceso

La autorización para tener acceso a la información computarizada debe estar evidenciada y proporcionada por un gerente que tenga la responsabilidad de asegurar el uso y monitoreo de la información que esta siendo accesada. Esta autorización debe ser dada directamente por el administrador de seguridad evitando errores o alteración a la información.

1.4 Revisión de Autorización de Acceso

Como cualquier otro control, los controles de acceso deben ser evaluados regularmente para asegurar que aún son efectivos. Cambios de personal, accesos mal intencionados o por negligencia, pueden impactar en la efectividad del control de acceso. Por esta razón, el administrador de la seguridad, con la asistencia

de los gerentes que proveen autorización de acceso, deben revisar los controles de acceso por lo menos una vez al año. Cualquier acceso que exceda la filosofía de "necesidad de conocer, necesidad de hacer" debe ser actualizada.

1.5 Conocimiento de la Seguridad

El conocimiento de los empleados sobre la importancia de la seguridad, necesita ser comunicada a través de la combinación de una política de seguridad, entrenamiento y reforzamiento posterior. El entrenamiento debe mejorar el conocimiento de los empleados de sus responsabilidades relativas a seguridad.

Estas responsabilidades incluyen:

- Custodia de identificaciones de usuarios y passwords
- Reportar sospechas de violaciones de seguridad al administrador de seguridad
- Lectura de la política de seguridad y
- Mantener una adecuada seguridad física, custodiando puertas, resguardando llaves de acceso, no publicar combinaciones de chapas de seguridad e identifcar y vigilar a personas no familiares

1.6 Reglas del Administrador de Seguridad

El administrador de seguridad, generalmente es un miembro del departamento de sistemas de información, es responsable de la implantación, monitoreo y ejecución de la reglas de seguridad establecidas y autorizadas por la dirección. Para proveer una adecuada segregación de funciones, esta persona no debe ser responsable de la actualización de datos de aplicaciones, o ser usuario final, programador de aplicaciones, operador o capturista.

1.7 Comité de Seguridad

La seguridad debe abarcar a toda la compañía. Representantes de todas las áreas de la compañía deberán reunirse para discutir los puntos de seguridad y establecer lineamientos sobre los mismos.

2 ACCESO FISICO

2.1 Elementos y Exposiciones Físicas y Ambientales

Las exposiciones físicas y ambientales podrían resultar en pérdidas financieras, repercusiones legales, pérdida de credibilidad o de competitividad, ello puede originarse por imprevistos naturales y hechos ocasionados por participación humana y pueden exponer el negocio a accesos no autorizados.

Desde el punto de vista de sistemas de información, las instalaciones a ser protegidas incluyen las siguientes: área de programación, área de cómputo, consola de operación, biblioteca de cintas, área de almacenamiento, instalación externa de respaldos, control de entradas y salidas del área de cómputo, gabinete de comunicaciones, equipo de telecomunicaciones, microcomputadoras, fuentes de poder, instalaciones de cómputo disponibles, impresoras locales y remotas y redes de área local.

Sin embargo, para que esta salvaguarda sea efectiva, debe extenderse no solo a la instalación de cómputo, si no a toda la organización. Puede incluir instalaciones remotas, rentadas o compartidas.

2.2 Eventos y Exposiciones Físicas

Las siguientes formas de acceso físico deben ser evaluadas para mantener una adecuada seguridad: todas las puertas de acceso, ventanas y paredes de cristal, sistemas de ventilación, y paredes falsas o sobrepuestas.

2.2.1 Exposiciones Físicas

Los riesgos que existen de una violación accidental o intencionada de estas formas de acceso incluyen:

- Acceso no autorizado
- Daños al equipo y mobiliario
- Vandalismo al equipo y mobiliario
- Robo de equipo, mobiliario y documentos
- Copias o inspección de información sensitiva
- Alteración de equipo de información sensitiva
- Revelación pública de información sensitiva
- Chantaje
- Desfalcos

2.2.2 Exposiciones Ambientales

Las exposiciones ambientales son primariamente debido a eventos ocurridos natural y fortuitamente. Sin embargo con controles adecuados las exposiciones a estos elementos pueden ser reducidos:

- Fuego
- Agua
- Variaciones de energía
- Daños estructurales
- Contaminación

2.3 Controles Físicos y Ambientales

Los controles físicos y ambientales son diseñados para proteger a la organización de hechos fortuitos y prevenir accesos no autorizados.

2.3.1 Controles Físicos

Los controles físicos deben limitar el acceso a individuos autorizados por la dirección. Esta autorización puede ser explícita, como una chapa de seguridad de la cual solo el gerente de sistemas cuente con llave; o implícita, como una descripción de trabajo (job description) que implica la necesidad de accesar reportes y documentos sensitivos.

Algunos dispositivos para prevenir el acceso no autorizado son:

- Cerraduras convencionales
- Cerraduras de combinación
- Cerraduras electrónicas
- Cerraduras biométricas
- Bitácoras de acceso
- Gafetes de identificación
- Cámaras de video
- Puerta única de acceso
- Sistema de alarma

2.3.2 Controles Ambientales

Los controles ambientales reducen el riesgo de interrupción de operaciones debido a los efectos adversos del medio ambiente. Estos factores ambientales incluyen: calidad del aire, energía eléctrica y condiciones del suelo y atmosféricas.

Fuego

El fuego es la mayor amenaza para la seguridad física de una instalación de cómputo, algunas de las principales características de un sistema de protección contra incendios bien diseñado son:

1. Alarmas de fuego automáticas y manuales localizadas en lugares estratégicos dentro de la instalación.

2. Un sistema automático de extinción que disperse el extintor apropiado: agua, bioxido de carbono, halón.

3. Los tipos apropiados de extinguidores manuales de fuego deben localizarse en lugares estratégicos dentro de la instalación.

4. Un panel de control que muestre donde se han activado las alarmas automáticas o manuales en toda la instalación.

5. Existencia de interruptores maestros de energía (incluyendo aire acondicionado) y del sistema automático de extinción, cerca del panel de control.

6. El edificio haya sido construído con materiales resistentes, y esté estructuralmente estable cuando ocurra un daño por fuego.

7. Extinguidores y salidas de emergencia claramente marcados.

El administrador de la seguridad debe planear inspecciones de todo el sistema de protección contra fuego. El uso apropiado de estos sistemas requieren entrenamientos y adiestramiento periódico del personal. Los procedimientos a ser seguidos durante una emergencia deben estar documentados.

Agua

Los daños por agua en una instalación de cómputo pueden ser resultado de una amenaza de fuego; los sistemas de extinción rocían agua que penetra en el equipo, o los conductos de agua pueden romperse. Por otro lado, los daños por agua resultan de otras fuentes: ciclones, tornados, nevadas.

Algunas de las mejores formas de proteger la instalación contra daños por agua son:

1. En donde sea posible, tener paredes, pisos y techos a prueba de agua.
2. Asegurar que exista un sistema de drenaje adecuado.
3. Instalar alarmas en puntos estratégicos dentro de la instalación.
4. En áreas de inundaciones tener la instalación arriba del nivel de agua.
5. Tener un interruptor maestro para todas las tuberías.
6. Usar un conducto de secado automático.

Variaciones de Energía

Las variaciones de energía toman la forma de incrementos, decrementos o pérdidas de poder. Los reguladores de voltaje protegen al hardware contra incrementos temporales de poder. Los interruptores automáticos protegen al hardware contra incrementos de voltaje prolongados. Las baterías proveen energía si existe una pérdida temporal de poder; sin embargo, una planta generadora es necesaria para pérdidas prolongadas de poder. El nivel de protección necesita depender de la habilidad y utilidad de la compañía para mantener una fuente de poder ininterrumpida y de la probabilidad que otro desastre ocurra (p. ej. terremoto) que destruya la fuente de poder.

La energía es necesaria no solamente para asegurar el funcionamiento del hardware si no también para mantener un medio ambiente que este libre de polvo y

relativamente constante con respecto a temperatura y humedad.

Daños Estructurales

Los daños estructurales a la instalación pueden ocurrir de varias maneras: terremotos, aironasos, nevadas, avalanchas. La prevención de desastres ocurridos por daños estructurales es principalmente una cuestión de ingeniería. En el diseño de un edificio, el peso de la estructura debe ser considerado en la construcción. Sin embargo, si un centro de cómputo esta localizado en el edificio, el diseño de ingeniería debe considerar los requerimientos estructurales especiales para el adecuado funcionamiento del centro de cómputo.

Si hay alguna elección en donde instalar el centro de cómputo, podría elegirse la zona menos propensa a que existan daños estructurales, por ejemplo, lejos de una zona de inundaciones o una región de alta actividad sísmica. Es recomendable instalar el centro de cómputo en un piso alto de un edificio, este sería menos suceptible de daños por inundaciones, y también el acceso no autorizado sería más fácil.

Contaminación

Para la continuidad de operaciones de una computadora se depende de un medio ambiente libre de contaminación. El mayor contaminante es el polvo. El polvo se acrecenta si no existe una adecuada filtración de aire que pasa a través del sistema del aire acondicionado o si se permite que éste se acumule en el equipo, pisos, etc. Amplios daños a un procesador central son resultado de alimentos, bebidas y cigarros ingresados en la instalación, además de provocar la creación de algunos contaminantes.

En general, la contaminación es minimizada adoptando procedimientos internos, estos procedimientos también facilitan el adecuado funcionamiento de la instalación. Algunos de ellos podrían ser: la prohibición de comer, beber y fumar dentro de la instalación.

3 ACCESO LOGICO

3.1 Vías de Acceso Lógico

El acceso lógico dentro del computador puede ser logrado a través de diversas vías. Esto debe estar sujeto a niveles apropiados de seguridad de acceso. Estos métodos de acceso incluyen los siguientes:

3.1.1 Consola de Operación

Esta terminal privilegiada controla las funciones y operaciones del computador central. Para proporcionar seguridad, estas terminales deben estar situadas en un centro de cómputo o una instalación debidamente controlada a través de acceso físico restringido, siendo esto un beneficio para operadores del computador y soporte al personal.

3.1.2 Terminales en línea

Este modo de acceso lógico es el más común entre usuarios. Normalmente, éste requiere para su acceso de un perfil de usuario y un password para acceso al computador. El acceso en línea permite tener un proceso de datos inmediato, pueden realizarse transacciones de acceso, consulta, y actualización de archivos (agregar, cambiar, borrar). Asímismo por ser un acceso inmediato, la necesidad de establecer seguridad lógica es indispensable. Esto es controlado a través de software de acceso.

3.1.3 Trabajos procesados en lotes

Este modo de acceso es indirecto, sin embargo, este acceso es logrado vía proceso de transacciones en grupo. Generalmente involucra transacciones de entrada acumuladas y procesos por lotes, dando intervalos de tiempo entre procesos. La seguridad es lograda por quien tiene el acceso al ingreso de datos (capturista) y quien inicializa los procesos por lotes (operadores del sistema o el sistema de calendarización de trabajos).

3.1.4 Exposición y consecuencias del acceso lógico

Los controles de acceso lógico incrementan la pérdida potencial de la organización, resultado de exposiciones técnicas y de negocio. Estas exposiciones resultan en inconvenientes menores o en una pérdida total de las funciones del computador.

3.2 Perpetradores de Acceso Lógico

Un perpetrador de acceso lógico es frecuentemente el mismo personal que tiene el poder de sacar partido de la situación. No obstante, el conocimiento práctico necesario para violar el acceso lógico es mas técnico y complejo.

3.2.1 Hackers

Comunmente los hackers intentan poner a prueba los límites de restricción de acceso, para demostrar su habilidad para vencer obstáculos. Estos usualmente no intentan destruir, pero frecuentemente esto sucede.

3.2.2 Empleados

- Personal de Sistemas.

  Estas personas tienen la facilidad de acceso a la información del computador ya que ellos son los que custodian esta información. Además del control de acceso lógico, es necesaria una buena segregación de funciones y supervisión que ayuden a controlar a este personal.

- Usuario Final.

3.2.3 Exempleados.

En particular, se debe ser cauteloso con los exempleados que hayan dejado a la organización en términos desfavorables.

3.2.4 Accidentes por desconocimiento

Quienes por desconocimiento se convierten en perpetradores o violadores.

3.2.5 Terceros Interesados

- Competencia
- Potencias extranjeras
- Crimen organizado

3.3 **Exposiciones de Acceso Lógico**

La exposición que existe por accidentes o intentos por conocimiento práctico de los controles de acceso lógico, son debilidades que incluyen:

3.3.1 Exposiciones técnicas

- Accesos no autorizados, implantación o modificaciones de datos y software

Esta exposición incluye código fuente oculto y modificaciones directas o indirectas de datos y programas. A continuación algunos nombres de exposiciones:

. Manipulación de Datos

Esto involucra cambios de datos dentro del computador, es el abuso más común porque solo requiere de conocimientos técnicos limitados y ocurre antes de que la seguridad del sistema pueda proteger los datos.

. Caballo de Troya

Esto involucra código malicioso oculto en un programa autorizado del computador. Este código

oculto será ejecutado cada vez que el programa autorizado se ejecute.

. Redondeo (rounding down)

Esto consiste en quitar pequeñas cantidades de dinero de una transacción o cuenta computarizada y desviar esta cantidad a la cuenta del autor del delito. El término redondeo se refiere a redondear quitando las fracciones de centavo y transfiriendo estas pequeñas fracciones a una cuenta no autorizada. Estas cantidades son tan pequeñas que raramente se notan.

. Técnica del salami

Esta técnica es similar a la técnica de redondeo, pero consiste en cortar pequeñas cantidades de dinero de una transacción o cuenta computarizada.

. Virus

Son programas que se reproducen y difunden de computadora a computadora, esto es a través de diskettes compartidos o mediante la transferencia lógica en líneas de telecomunicaciones.

Algunos de los tipos de virus existentes son:

* Los simples

Son aquellos que, en cuanto entran al equipo, proceden a borrar información (programas y/o archivos), ya sea del disco duro o de cualquier medio magnético.

* Los temporales

Son aquellos que esperan una determinada fecha o que transcurra un cierto número de días para actuar.

* Los misteriosos

Aquellos que bloquean ciertos componentes del equipo (normalmente buffers) de manera que no puede entrar o salir información de los discos, apareciendo el mal, a primera vista, como una "falla de hardware".

* Los físicos

Aquellos que son capaces de dañar físicamente al equipo. Actualmente se conocen dos tipos: los que ocasionan daños a los monitores y los que ocasionan la "caída" de las cabezas de lectura y grabación sobre los discos, provocando que éstos se rayen y en consecuencia queden inservibles.

* Los creídos

Aquellos que cada vez que se ejecuta el programa, marcan sectores dañados en los discos (sin ser esto real), disminuyendo poco a poco su capacidad de almacenamiento.

* Los viajeros

Son los que viven en redes de equipos y tienen la habilidad de transmitirse entre un equipo y otro, pudiendo hacerlo por cualquier medio de comunicación de datos, tales como teléfono, microondas y satélite.

. Bombas de tiempo

Son similares a los virus, pero estos no se reproducen.

- Shut down de la computadora

Puede iniciarse el apagado del computador por conexiones directas (on-line) o indirectas (líneas de telemarcaje) de terminales. Frecuentemente para ello se requiere tener acceso a una identificación

de acceso de alto nivel. No resulta tan difícil si los controles de acceso correctos no están implantados alrededor de las identificaciones y las conexiones de telecomunicaciones con el computador.

- Interrupción del servicio.

  Las líneas de telecomunicaciones son vulnerables a la temperatura o cortes accidentales.

3.3.2 Exposiciones del negocio

Los delitos informáticos con el fin de aprovechar el computador y la información que contiene puede ser dañino para la reputación, la moral y la existencia de una organización. El resultado puede consistir en la pérdida de clientes, una situación embarazosa para la gerencia y el inicio de acciones legales contra la organización. Entre las amenazas para la organización se cuentan:

- Pérdidas financieras

  Pueden ser directas, por la pérdida de fondos electrónicos o indirectas, a causa de los costos de corregir la exposición al riesgo.

- Repercusiones legales

  Existen numerosas leyes que protegen los derechos a la privacidad que deben ser tomados en cuenta por la organización en la etapa de desarrollo de las políticas y procedimientos de seguridad. Estas leyes pueden proteger a la organización, pero también proteger de juicios al causante. El auditor debe recurrir a asesores calificados cuando procede hacer un examen de las cuestiones relacionadas con la seguridad informática.

- Pérdida de credibilidad o margen de credibilidad

  Muchas organizaciones, en especial las empresas de servicios como los bancos, entidades de ahorro y préstamo o inversiones, necesitan una alta

credibilidad y confianza del público para mantener su competitividad o incluso seguir funcionando. Una violación a la seguridad puede dañar gravemente esa credibilidad, con la consiguiente pérdida de negocios y prestigio.

- Chantaje/Espionaje industrial

Al obtener el acceso a la información confidencial o los medios para lograr un impacto adverso sobre las operaciones del computador, un perpetrador puede exigir a la organización pagos o servicios bajo amenazas de aprovechar la brecha en la seguridad.

- Sabotaje

En algunos casos no se busca una ganancia financiera, si no que simplemente mueve el deseo de realizar daño. Puede darse cuando el causante odia a la organización o simplemente desea un reto contra el cual enfrentarse.

3.4 Controles de Acceso lógico

Los archivos del computador deben ser protegidos de accesos innecesarios o no autorizados, mediante controles que reduzcan el riesgo de un mal uso intencional o no intencional, robo, alteración o destrucción.

En un ambiente de procesamiento en lotes (batch), este control puede obtenerse mediante la restricción y monitoreo de las actividades del operador de la computadora.

En un sistema en línea (on-line), las posibilidades de acceso son mas complejas y directas y el nivel de control debe ser por consiguiente más complejo, éstos controles de acceso necesitan ser aplicados, no sólo a operadores del computador, sino también a usuarios finales, programadores, administradores de seguridad, gerencia y cualquier otra persona que pueda utilizar el computador, incluyendo personal externo.

3.4.1 Instalaciones y archivos del computador que deben ser protegidos a través de los controles de acceso lógico.

- Datos
- Software de aplicación
  . Pruebas y
  . Producción
- Utilerías
- Líneas de telecomunicaciones
- Bitácoras
- Bitácora de password
- Archivos temporales en disco
- Archivos en cinta
- Software del sistema
- Software de control de acceso
- Procedimientos del bibliotecario
- Sistemas operativos
- Directorios y diccionario de datos
- Líneas de comunicaciones

4 CONTINUIDAD DE OPERACIONES

Es necesario analizar y evaluar las políticas y procedimientos concernientes al plan de contingencias para asegurar la viabilidad de la organización, para responder efectivamente a desastres y otras situaciones de emergencia.

Cuando se revisa la continuidad de operaciones, las tareas del auditor de sistemas incluyen:

- Evaluar el plan de contingencias para determinar su funcionalidad y actualización, revisandolo y comparándolo con los estándares apropiados.

- Verificar que el plan de contingencias es efectivo para asegurar que la capacidad de proceso de información puede ser reactivada prontamente después de una interrupción no anticipada, revisando los resultados de pruebas previas llevadas a cabo por el personal del área de sistemas.

- Evaluar el almacenamiento externo, para asegurar su funcionalidad, mediante la inspección de la instalación, revisando su contenido y controles ambientales y de seguridad.

- Evaluar la viabilidad del personal de sistemas y usuarios para responder efectivamente ante situaciones de emergencia, revisando procedimientos de emergencia, entrenamiento a empleados y resultados de pruebas y simulacros.

4.1 Evaluación de Riesgos

La evaluación de riesgos involucra la priorización de sistemas, de acuerdo a la significatividad, a lo crítico de las operaciones que se manejan y al tiempo que se invierte, esto es necesario para la reanudación del negocio después de un desastre. La identificación de sistemas críticos resulta de un análisis de riesgos que se basa en la tolerancia dentro de la clasificación de sistemas, conteniendo las siguientes clasificaciones:

Críticos.- Incluyen las funciones que no pueden llevarse a cabo mediante métodos manuales, sino únicamente bajo un ambiente idéntico al existente. La tolerancia para interrupción es baja y el costo es muy alto.

Vitales.- Estas funciones pueden ejecutarse manualmente pero solamente por un breve periodo de

tiempo. Hay una mayor tolerancia a interrupciones que en los sistemas críticos, sin embargo, un bajo costo de interrupción prevee que las funciones sean realizadas dentro de cierto tiempo (generalmente 5 días o menos).

No Críticos.- Estas funciones pueden ser interrumpidas por un periodo de tiempo largo, con un pequeño o nulo costo para la compañía.

4.2 Seguros

El aseguramiento del proceso de datos es un asunto complejo. Existen pocas políticas estándar y usualmente una organización debe negociar las especificaciones de un contrato con una compañía de seguros. El gerente a cargo de la seguridad debe asegurarse que las siguientes áreas sean cubiertas:

Equipo e Instalación.- Donde deben ser cubiertos los daños físicos a las instalaciones de cómputo abarcando la reconstrucción del cuarto de cómputo, los sobrepisos, mobiliario especial y al propio equipo, incluyendo la reparación o adquisición de hardware.

Medios de Almacenamiento.- Cubriendo el reemplazo de los medios de almacenamiento más su contenido (archivos de datos, programas, documentación). El seguro debe estar disponible para situaciones dentro de las instalaciones, en otras instalaciones ó en tránsito y cubrir el costo actual de reproducción, considerando en la determinación del monto a cubrir los costos de programación para reproducir el medio dañado, el reemplazo del medio de almacenamiento y los gastos de respaldo.

Gastos Adicionales.- Deben cubrirse los costos adicionales incurridos porque la organización no esta operando desde sus instalaciones normales y necesita establecer un ambiente temporal de operaciones.

Interrupción de Relaciones Comerciales.- Cubriendo el reembolso de pérdidas monetarias resultantes de la suspensión de operaciones por la pérdida de equipo y/o información relevante para la obtención de beneficios.

Registros y Papeles que Representan Valores.- Cubren documentos fuente, reportes preimpresos, documentación y papeles que representan valores.

Errores y Omisiones.- Debe proveerse protección contra el riesgo legal en el que se pueda incurrir durante la práctica profesional al cometer un acto, error u omisión que resulte en pérdida financiera de un cliente. Este seguro fué originalmente diseñado para centros de servicio, pero ahora esta disponible para proteger a analistas de sistemas, diseñadores de software, programadores y consultores.

Cuentas por Cobrar.- Cubriendo los problemas de efectivo que se tengan porque la organización no puede recolectar sus cuentas por cobrar en un periodo corto de tiempo.

4.3 Plan de Contingencias

El propósito de un plan de contingencias es minimizar las consecuencias potenciales de una pérdida de la capacidad de proceso de datos por un amplio periodo de tiempo. El alcance de un plan de contingencias esta limitado a aquellos sistemas que son críticos y vitales para un negocio, incluyendo los sistemas existentes y los próximos a implantar. Uno de los pasos significativos en el plan de contingencias es la identificación de esas aplicaciones.

El plan debe estar dirigido no solamente a la recuperación de un desastre si no también a prevenir la ocurrencia de alguno como primer paso. Adicionalmente, tener un plan de contingencias no es suficiente para asegurar que será efectivo en el momento que ocurra un desastre, el plan debe ser continuamente actualizado y probado para asegurar que continúe reflejando los requerimientos de la organización y mantenga su efectividad.

Existen 8 puntos que deben cubrirse en la preparación de un plan de contingencias:

- Contar con un comité de alta dirección y designar un responsable del plan
- Evaluar los riesgos y estimar la pérdida potencial

- Establecer prioridades entre las aplicaciones automatizadas
- Determinar el mínimo de recursos requeridos
- Establecer el mejor método de recuperación
- Desarrollar el plan detallado
- Prueba del plan
- Mantenimiento del plan

Cada uno de estos pasos es descrito a continuación.

4.3.1 Contar con un Comité de Alta Dirección y Designar un Responsable del Plan

Esta actividad es la clave de todo el proceso. El plan de contingencias requiere inicialmente un monto significativo de recursos y un esfuerzo contínuo en lograr mantenerlo actualizado. Muchas de las decisiones tomadas afectan al negocio por completo, por eso demanda una participación substancial de la alta dirección. La persona responsable del proyecto debe ser capaz de dirigir las expectativas de la alta dirección y debe preferentemente no ser un empleado de proceso de datos, ya que estos tienen el conocimiento técnico, dependen de los sistemas automatizados y pueden pugnar por una sobrevaluación del impacto de la interrupción de los sistemas en términos del negocio, al evaluar las expectativas de la alta dirección. Este es un paso que la organización debe evaluar si tiene los suficientes recursos experimentados para el proyecto o si necesita asistencia de recursos externos. Como todos los proyectos, el equipo debe ser seleccionado cuidadosamente, esto incluye tanto usuarios como personal de proceso de datos, para lo cual es necesario proporcionar un adecuado entrenamiento.

4.3.2 Evaluar los Riesgos y Estimar la Pérdida Potencial

Esta es una fase extensa y difícil, en la que se actúa con incertidumbre y es necesaría la aplicación del criterio. Muchas compañías están preparadas para aceptar altas probabilidades de ocurrencia de amenazas, donde las consecuencias son menores o de igual manera si las consecuencias fueran catastrófi-

cas para la compañía, ya que normalmente se cree que la probabilidad de ocurrencia es casi nula.

Algunas compañías, sin embargo, están preparadas para aceptar mayores riesgos que otros, dependiendo de su filosofía general con respecto a los riesgos. Las acciones que se toman pueden ser pensadas como una serie de protecciones:

- Medidas preventivas para reducir la probabilidad de amenazas
- Medidas de detección/recuperación para reducir las consecuencias de la amenaza
- Seguros para recuperar los costos incurridos

El factor determinante es la capacidad del negocio para absorber las pérdidas.

La planeación de contingencias es frecuentemente considerada por separado de la discusión de medidas preventivas, estas últimas deben ser consideradas y examinadas durante ésta fase.

Las amenazas a los sistemas automatizados necesitan ser identificadas y la probabilidad de ocurrencia determinada. Esta probabilidad de ocurrencia depende del nivel de defensas ya introducidas. No es necesario preparar un probabilidad precisa, una evaluación un poco más subjetiva de si la probabilidad es alta, media o baja, puede ser hecha. Con base en ella se decidirá cuanto se esta preparado para gastar en la reducción del riesgo de ocurrencia o para recuperarse de las consecuencias de la amenaza. Esta tarea requiere un alto nivel de conocimientos acerca del negocio para asegurar que todos los efectos son considerados.

4.3.3 Establecer Prioridades contra las Aplicaciones Automatizadas

El plan de contingencias debe solamente dirigirse a los sistemas críticos y vitales de aplicación. Estos son los sistemas considerados indispensables en términos de importancia para la sobrevivencia comercial del negocio. Muchas aplicaciones sobrepasan los límites departamentales, haciendo con ello más

difícil la determinación de todas las consecuencias al no tener un sistema de aplicación disponible.

Para cada aplicación debe hacerse una estimación de cuanto tiempo la organización puede estar sin ella, así como los costos que esto implicaría.

4.3.4 Determinar el Mínimo de Recursos Requeridos

Este paso debe realizarse acto seguido al establecimiento de prioridades, esta es una fase muy técnica y probablemente sea dirigida por el departamento de proceso de datos. Involucra la determinación de la cantidad de memoria, espacio en disco, líneas de telecomunicaciones y fuente de poder requerida para procesar las aplicaciones esenciales. Es importante asegurar que el espacio en disco requerido sea identificado cuidadosamente. Esto, por ejemplo, por que puede ser necesario restaurar en una instalación temporal todos los archivos históricos asociados con una aplicación crítica.

4.3.5 Establecer el Mejor Método de Recuperación

La identificación de la más apropiada opción es relativamente fácil, algunas de las opciones se explican a continuación.

No hacer nada

Esto significa, atenerse a la cobertura de seguros, sin embargo, esto es válido si la póliza de seguros cubre todas las actividades realizadas por el área de proceso de datos, así como la información y relaciones comerciales.

Fortress Approach

Este método de recuperación normalmente se combina con alguna de las otras opciones. El énfasis se centra en la prevención de la ocurrencia de un desastre, esto significa que los controles tienen que ser muy herméticos en el medio ambiente de seguridad, a tal grado que el centro de cómputo se asemeja a una fortaleza.

Centro de Recuperación Básico (Cold SITE)

Estos son los centros de recuperación que cuentan con el medio ambiente básico (instalación eléctrica, aire acondicionado, sobre piso, principalmente) para que pueda operar una instalación de proceso de datos. El centro de recuperación básico esta listo para recibir equipo, pero no ofrece ningún componente adicional. La activación del centro puede tomar varias semanas.

Centro de Recuperación Portátil (Portable Backup Centre)

Es similar al centro de recuperación básico, pero basado en unidades modulares que pueden ser localizados en sus instalaciones.

Centro de Recuperación Medio (Warm SITE)

Son los centros de recuperación que estan parcialmente configurados, usualmente con equipos periféricos, tales como unidades de disco , unidades de cinta y controladores, pero sin computadora central. En algunas ocasiones un centro de recuperación medio esta equipado con un pequeño CPU. Después de la instalación de los componentes no contemplados, el centro estará listo para funcionar en pocas horas, sin embargo, la localización e instalación del CPU y otras unidades adicionales puede tomar varios días o semanas.

Convenio Mutuo de Respaldo (Mutual Backup Arrangement)

Se refiere a arreglos recíprocos que son frecuentemente informales. El equipo y sistema operativo deben ser compatibles y cada parte en el convenio debe tener suficiente capacidad económica para procesar sus sistemas y los sistemas clave de la otra parte en el convenio. Es difícil el soporte a otra compañía por la capacidad de espacio disponible, ya que este espacio se utiliza por los desarrolladores. Los arreglos informales por consiguiente no son convenientes y legalmente los contratos son difíciles de acordarse.

Centro de Recuperación Completo (Hot SITE)

Es un centro de recuperación completamente configurado y listo para operar en pocas horas. El equipo y software de sistemas debe ser compatible con la instalación primaria a ser respaldada. Los recursos adicionales necesarios son el personal, programas y archivos de datos.

Operaciones en Centros Múltiples

Esta opción esta incrementándose para compañías con sistemas distribuidos y redes. La falla de un centro de procesamiento puede ser compensado con la instalación de sus programas en otro nodo de la red. Las dificultades son normalmente en el almacenamiento de los archivos de datos en diferentes centros y como consecuencia la degradación en el tiempo de respuesta y en asegurar que la suficiente capacidad este siempre disponible.

4.3.6 Desarrollar el Plan Detallado

Habiendo finalizado la estrategia en la fase previa y obtenida la aprobación de la dirección, la fase más extensa inicia. Los procedimientos detallados necesitan ser diseñados para las siguientes actividades:

- Recuperación de aplicaciones
- Recuperación de la instalación de cómputo
- Recuperación de personal
- Ejecución del Plan de Contingencias

Procedimientos de Recuperación de Aplicaciones

Esta función debe llevarse a cabo por separado en cada aplicación considerada crítica. Los perfiles de cada aplicación deben ser definidos primeramente de la documentación existente. Esto cubrirá generalmente la aplicación en términos de archivos, bases de datos, procesos, operación y requerimientos a proveedores, balanceo de procedimientos y

distribución. Los requerimientos en términos de software, espacio en disco y equipo, deben ser identificados así como los procedimientos de respaldo de datos, programas y software de sistemas, de esta manera, será sencillo durante cualquier desastre poder reestablecer sus operaciones en una instalación alterna dependiendo de que tan reciente es el último respaldo. Los procedimientos de recuperación, incluyendo cualquier procedimiento de arranque/reinicio, deben también ser definido.

En muchos casos, la información previamente indicada ya se tiene especificada dentro de los manuales de operación y por lo tanto solo necesitan confrontarse. Sin embargo, si solo ciertos elementos o subsistemas dentro de la aplicación general han sido identificados como críticos, es necesaria su modificación. Estos requerirán pruebas para segurar que ellos son efectivos y que no omiten ninguna relación crítica en otros sistemas.

Procedimientos de Recuperación de la Instalación de Cómputo

Inicialmente, un perfil de los requerimientos de instalación debe ser definido por cada aplicación, y entonces agregado dentro de un requerimiento general. Los requerimientos deben cubrir hardware, software de sistemas y utilerías, comunicaciones y proveedores de cómputo. Existen métodos alternativos que deben ser identificados.

En esta fase existen contratos, los cuales deben ser examinados, almacenamientos de respaldo fuera del centro de procesamiento, determinación de proveedores, procedimientos de mantenimiento de equipo los cuales deben ser revisados así como tener contactos actualizados.

Las pautas a seguir en un desastre y grados de emergencia deben ser definidos. La responsabilidad para la declaración de emergencias debe ser distribuida y las acciones subsecuentes identificadas. Los procedimientos de monitoreo de situaciones son obligados.

Procedimientos de Recuperación de Personal

En esta fase es donde se requiere se identifiquen las habilidades del equipo de contingencias y que las tareas asignadas a individuos sean de acuerdo a estas. En cada caso, deben ser nombrados suplentes para situaciones de falta de disponibilidad del titular. Entrenamiento adicional es requerido para que cada persona obtenga una adecuada habilidad. Es necesario que el personal usuario requerido forme parte del equipo tanto como el personal de proceso de datos involucrado en operación, telecomunicaciones, mantenimiento de hardware y software, además del personal de soporte administrativo. Una persona debe también ser reponsable de la coordinación con clientes, empleados y otras personas afectadas por el desastre, esto es muy importante para mantener credibilidad y lealtad, lo cual sólo se logra a través de una comunicación positiva.

Ejecución de Procedimientos

Esta actividad involucra la definición de procedimientos y pautas a seguir en la decisión de poner en operación el plan de contingencias. Los procedimientos deben identificar quien es la autoridad para declarar un desastre. Esta persona debe ser un miembro de la alta dirección, quien también debe detallar el paso inicial de notificación a los miembros del equipo de contingencias y contactar con los principales proveedores.

La falta de instrucciones claras puede demorar significativamente o impedir el proceso de recuperación. Los procedimientos deben ser plasmados simple y categóricamente, la ambigüedad e inestabilidad causan confusión.

El Documento

El plan de contingencias debe contener las siguientes secciones:

- Generalidades del Plan

  Incluye el alcance del plan y la estrategia general que esta siendo adoptada

- Acciones dentro del Modo de Recuperación de Desastres

  Se deben mostrar delineados los procesos por medio de los cuales la dirección decide activar el plan de contingencias y proveer un plan de trabajo general especificando tareas y responsabilidades.

- Instalación de Sistemas Críticos en el Centro de Recuperación de Desastres

  Deben indicarse los procedimientos para notificar al centro de recuperación, la obtención del software del centro de respaldo fuera del centro de procesamiento y su instalación en el centro de recuperación, además de la manera de obtener los dispositivos críticos y la transportación adecuada.

- Ejecutar Operaciones de Recuperación

  Indicándose el calendario de producción, sometimiento de trabajos, uso de terminales, requerimientos de trabajo y distribución de reportes, mientras se ejecutan los sistemas críticos en el centro de proceso propio.

- Recuperación de Operaciones en el Centro de Proceso Propio

  Preparación del centro de procesamiento para restaurar la capacidad de proceso de datos, reemplazo de hardware, software de sistemas y de aplicación, telecomunicaciones, reanudar el proceso

de producción y ponerse al día con el soporte de procesamiento.

- Coordinación de Usuarios y Contabilidad

Deben mostrarse los procedimientos para notificar a los usuarios, asegurando que ellos tengan los procedimientos de contingencia basados en un manual de actividades, la coordinación con ellos y el registro de costos por reclamación de seguros.

- Prueba y Mantenimiento del plan

Los procedimientos y responsabilidades para probar y mantener el plan deben estar claramente identificados y el plan debe distribuirse y darse a conocer.

4.3.7 Prueba del Plan

Durante un desastre real, existen demasiados problemas y dolores de cabeza sin saber porque el plan básico y los procedimientos no están trabajando. Por lo tanto el plan debe porbarse hasta que éste muestre su efectividad; pruebas periódicas al menos una vez al año deben darse para asegurar que continúa reflejando los requerimientos de la organización. Las pruebas deben ser cuidadosamente planeadas para que todo el personal pueda involucrarse potencialmente en un desastre real, teniendo con ello el personal, experiencia en los procedimientos de recuperación. La rotación de personal ayuda a asegurar que los procedimientos están propiamente documentados y no depender del conocimiento de algunas personas en particular. Observadores deben vigilar por cada prueba, que todos los eventos importantes queden registrados en la forma en que sucedieron y retroalimentar las revisiones del plan de contingencias.

4.3.8 Mantenimiento del Plan

La responsabilidad para el mantenimiento del plan debe ser asignada. La planeación de contingencias es improbable que sea una actividad de tiempo completo después de haber completado satisfactoriamente la prueba del plan. Por lo tanto es apropiado establecer mecanismos dentro de los procedimientos diarios para

actualización del plan para toda la organización. La persona responsable del plan debe también asegurarse que la planeación de contingencias es considerada en todos los nuevos desarrollos de sistemas y que los departamentos usuarios guarden su propio plan de contingencias actualizado.

CAPITULO V

SISTEMAS DE APLICACION

V. SISTEMAS DE APLICACION

OBJETIVO

Identificar, analizar y evaluar las debilidades, fortalezas, eficiencia y efectividad de los componentes dentro de los sistemas de aplicación.

La forma de lograr este objetivo es mediante:

- La identificación de las aplicaciones significativas y el flujo de transacciones de los sistemas para obtener un entendimiento detallado de las aplicaciones a revisión, así como la documentación disponible y las entrevistas con el personal apropiado.

- La identificación de la fortaleza de los controles de aplicación y evaluación del impacto de las debilidades de control para el desarrollo de pruebas estratégicas para analizar la información acumulada.

- La verificación de controles para asegurar su funcionalidad y efectividad mediante la aplicación de procedimientos adecuados de auditoría.

- La evaluación del ambiente de control para determinar que los objetivos de control se estén llevando a cabo a través del análisis del resultado de las pruebas y otras evidencias de control.

- La consideración de aspectos operacionales de las aplicaciones para asegurar que estos sean eficientes y efectivos mediante la comparación de los sistemas con los estándares de programación y los procedimientos de análisis utilizados comparándolos con los objetivos gerenciales del sistema.

INTRODUCCION

Los controles de aplicación se refieren a las funciones de control sobre entradas, procesos y salidas. Los controles de aplicación incluyen:

- Métodos para asegurar que solamente se ingresen y actualicen datos completos, precisos y validos.
- Procesos que lleven a cabo las funciones correctas.
- Procesos que obtengan los resultados esperados.
- Mantenimiento de datos.

Estos controles consisten en pruebas de edición, totales, conciliaciones e identificación y reporteo de datos incorrectos o de excepción. Los controles automatizados deben ser incluídos dentro de manuales de procedimientos para asegurar la apropiada investigación de excepciones.

1 AMBIENTE DE SISTEMAS DE APLICACION

Las funciones de operación son automatizadas con el propósito de mejorar la eficiencia e incrementar la confiabilidad de la información. Estas aplicaciones incluyen normalmente contabilidad general, pago de nóminas, cuentas por pagar, para la industria especificamente. Así como, préstamos bancarios, hipotecarios y depósitos para instituciones bancarias. Estas aplicaciones en un ambiente de sistemas, hacen más complejos los esfuerzos de auditoría, dado que su única característica incluye pistas de auditoría limitadas, actualización instantánea y sobrecarga de información.

Los sistemas de aplicación residen en varios ambientes incluyendo:

1.1 Sistema de Punto de Venta (POS)

Facilita la captura de datos en el tiempo y lugar donde se originan las transacciones. Las terminales de punto de venta incluyen el uso de lectores ópticos (scanners) para el uso de código de barras o lectura de tarjetas magnéticas para usarse con tarjetas de crédito. El sistema de punto de venta esta en línea con un computador central o es posible usar terminales independientes (stand-alone) o microcomputadoras para mantener las transacciones hasta el final de un periodo específico, cuando estos son enviados al computador central para ser procesados en bloque (batch).

1.2 Sistema de Manufactura Integral

Esta aplicación esta diseñada para ayudar en el mantenimiento del balance de inventarios para proporcionar el máximo nivel de servicio. El sistema puede ser usado para datos históricos, pronósticos y análisis de clientes. Incluye actividades de inventarios, registro de nuevos materiales, archivos de producción en proceso, archivos de producto terminado y ajustes. Compras, Ventas, Cuentas por pagar, cuentas por cobrar, recepción de mercancías y facturación pueden ser incluídas. Algunos sistemas integrales pueden combinar controles manuales con funciones automatizadas.

1.3 Intercambio Electrónico de Datos

Es la transmisión electrónica de documentos en un intercambio de formatos estándares entre dos organizaciones. El intercambio electrónico de datos, promueve aún más el uso eficiente de papeles.

La transmisión puede sustituirse con el uso de estándares de documentación incluyendo facturas y ordenes de compra.

1.4 Transferencia Electrónica de Fondos

Es el intercambio de dinero vía telecomunicaciones, EFT (Electronic Funds Transfer) se refiere a cualquier transacción financiera que se origina en una terminal y que transfiere una cantidad de dinero de una cuenta a otra.

1.5 Archivo Integrado de Clientes

El archivo integrado de clientes proporciona todos los detalles referentes a las relaciones comerciales que un cliente mantiene con una organización. La integración de todos los archivos ayuda en el análisis de clientes y en mercadotecnia. Un ejemplo de un archivo integrado de clientes incluye algunos archivos de clientes de bancos, este archivo mantiene todos los datos respecto de una cuenta de un cliente que pueden ser préstamos, cuentas de cheques, cuentas de inversión y cualquier certificado de depósito.

1.6 Automatización de Oficinas

Actualmente muchas oficinas aprovechan la variedad de dispositivos electrónicos. Los procesadores de palabras, microcomputadoras y correo electrónico son utilizados diariamente. Las LAN's (Redes de área local, Local Area Network) proporcionan una liga hacia otras oficinas y en muchas ocasiones acceso a las ligas con mainframes. Sin embargo, las LAN's pueden contener datos vitales y los controles de acceso suelen ser débiles.

2 PROCEDIMIENTOS DE CONTROL DE ENTRADA

Los procedimientos de control de entrada aseguran que todas las transacciones que serán procesadas se recibieron, procesaron y registraron adecuada y totalmente. Estos controles pueden también asegurar que únicamente información autorizada y validada es procesada.

2.1 Autorización de Entrada

La autorización de entrada verifica que todas las transacciones (operaciones) han sido adecuadamente autorizadas por la gerencia.

Algunos tipos de autorización incluyen :

- Firma de formatos batch proporciona evidencia de una adecuada autorización.

- Control de acceso en línea asegura que exista una adecuada autorización individual para el acceso de información.

- Passwords únicos son necesarios para asegurar que la autorización de acceso no puede ser expuesta a través del uso de otra autorización de acceso individual a la información.

  Los passwords individuales también proprocionan la responsabilidad para hacer cambios de datos.

- Documentos fuente son las formas usadas para el registro de datos. Un documento fuente es una hoja de papel, un documentocon datos preimpresos o una imágen desplegada de datos de entrada en línea.

  Un documento fuente bien diseñado logra varios propósitos: incrementa la rapidez y precisión con la que la información puede ser registrada, control sobre el flujo de trabajo, facilita la preparación de información para lectura en dispositivos de reconocimiento de formatos establecidos, incrementa la rapidez y precisión con que la información puede

ser leída y facilita por consecuencia la verificación de referencias.

Los documentos fuente deben ser formas preimpresas para proporcionar consistencia, precisión y legibilidad, deben incluir encabezado, título, notas e instrucciones.

El diseño del documento fuente debe:

- Enfatizar la facilidad de uso y ser legible.
- Crear grupos similares en campos unidos para facilitar el ingreso.
- Proporcionar códigos de entrada predeterminados para reducir errores.
- Contener marcas apropiadas, números de referencia o una identificación comparable para facilitar la búsqueda.
- Uso de recuadros para identificar el tamaño del campo.
- Incluir un área apropiada en el documento para la autorización por parte de la gerencia.

Todos los documentos fuente deben ser adecuadamente controlados. Los documentos fuente en blanco no deben estar en custodia del personal que origina las transacciones (operaciones) que estén asociadas con el uso de esta documentación.

Si los documentos fuente no están prenumerados, se deben establecer procedimientos para asegurar que todos ellos han sido considerados e ingresados.

2.2 Edición y Validación de Información

La validación de información indentifica datos erróneos incompletos o extraviados, así como inconsistencia entre los datos relacionados.

Tipos de edición y validación de información:

- Control secuencial.- El control numérico sigue una secuencia y cualquier número fuera de ella es rechazada o registrada en un reporte de excepción para darle el seguimiento correspondiente. Por ejemplo: las facturas son numeradas secuencialmente, la facturación del día comienza con la 12001 y termina con la 15045, si alguna factura mayor que la 15045 es encontrada durante el proceso debe ser rechazada como un número de factura inválido.

- Control de límites.- La información no debe exceder un monto predeterminado, por ejemplo: un cheque no debe exceder a $4,400.00, si un cheque excede este monto la información será rechazada para su posterior investigación.

- Control por rangos.- La información debe caer dentro de un rango predeterminado, por ejemplo: la clave por tipo de productos tiene un rango de 100 a 245, si alguna clave esta fuera de este rango debe ser rechazada como un código de producto inválido.

- Control de paridad.- Son bits sin información agregados para formar datos, la suma siempre da un número non o par, esto hace que el total de datos recibidos sea igual al total de datos agregados o transmitidos.

- Control de validez.- Verificar la programación de la validación de datos de acuerdo a criterios predeterminados, por ejemplo: el registro de pagos contiene un campo para estado civil. Las claves aceptables son (C) casado o (S) soltero, si cualquier otra clave es ingresada el datos debe ser rechazado.

- Búsqueda en tablas.- El ingreso de información esta de acuerdo a criterios predeterminados contenidos en una tabla, por ejemplo: el código de ciudad de 1 a 10 es ingresado por el empleado encargado. Este número debe corresponder a los establecidos en la tabla, relacionando el código al nombre de la ciudad.

- Dígito verificador.- Es un valor numérico el cual ha sido calculado matemáticamente y agregado al dato original para asegurar que la información no ha sido alterada o que una incorrecta pero válida relación ha ocurrido, este control es efectivo detectando errores de trasposición. Por ejemplo un dígito verificador es ingresado en un número de cuenta para asegurar la validación de la cuenta.

- Verificación de totalidad.- Un campo debe siempre contener datos y no ceros o blancos, un chequeo de cada byte de ese campo debe ser efectuado para determinar si algún dato no esta en blanco o en ceros. Por ejemplo: el número del seguro social en el registro de un nuevo empleado se deja en blanco. Esto se identifica como una llave de campo y el registro debe, por lo tanto, ser rechazado, pidiendo que ese campo sea completo antes que el registro sea aceptado para su prccesamiento.

- Verificación de duplicados.- Las transacciones se relacionan hacia aquellas ya ingresadas para asegurar que no se hayan ingresado anteriormente.

2.3 Balanceo y Control de Lotes

El control manual de lotes agrupa transacciones de entrada para proporcionar totales de control. El control de lotes puede basarse en totales monetarios, totales de movimientos, totales de documentos o hash total.

Tipos de control de lotes :

- Totales monetarios.- Verifican que el total de valores monetarios de los elementos a procesarse sea igual al valor total de los documentos en el lote. Por ejemplo: El valor total de las facturas por venta están acordes con el total del lote de las facturas procesadas por venta.

- Total de movimientos.- Verifican que los totales numéricos de movimientos incluyendo cada uno de los documentos en el lote estén acorde con el total numérico de los movimientos procesados.

- Total de documentos.- Verifican que el número total de documentos en el lote sea igual al número total de documentos procesados. Por ejemplo: que el número total de facturas en el lote estén acorde con el total de facturas.

- Hash total.- Verifica que un campo numérico predeterminado exista para todos los documentos en un lote, y sea acorde al total de documentos procesados.

El balanceo de lotes se ejecuta considerando ajustes manuales o automáticos. El total del lote debe ser combinado con los procedimientos adecuados de seguimiento de diferencias.

Deben existir controles adecuados para asegurar que las transacciones creadas se encuentren en un documento de entrada, que la totalidad de los documentos están incluidos en un lote, que todos los lotes sean enviados a proceso, que todos sean aceptados por el computador, que se lleven a cabo la verificación de totales por lote, los procedimientos para la investigación y tiempo de corrección de diferencias, así como los controles de reingreso de datos rechazados.

Tipos de balanceo de lotes:

- Registro por lote.- Facilita el registro manual de totales por lote.

- Control por cálculo.- Son ejecutados a través del uso de un archivo de edición para determinar el total del lote. Los datos son entonces procesados hacia el archivo maestro y una conciliación se ejecuta entre los totales procesados durante el archivo de edición inicial y el archivo maestro.

- Ajustes automáticos.- El ajuste automático del total del lote es ejecutado a través del uso del encabezado del lote, donde el total calculado es registrado.

2.4 Reporte de Errores de Entrada

Los controles para verificar que los datos son aceptados dentro del sistema correctamente, deben incluir el manejo de la corrección de errores de entrada.

El manejo de errores de entrada puede ser procesado por:

- Reingreso de transacciones con error.- Unicamente transacciones que contienen error deben ser rechazadas, el resto de los lotes correctos deben ser procesados normalmente.

- Rechazo de todo el lote de transacciones.- Cualquier lote que contenga errores debe ser rechazado para su corrección, previa al proceso.

- Aceptación de lotes en suspenso.- Cualquier lote con error no debe ser rechazado, sin embargo, el lote debe ser identificado para suspensión pendiente de corrección.

- Aceptación de lotes y señalamiento de transacciones erróneas.- Cualquier lote que contenga error debe ser procesado; sin embargo, esas transacciones con error deben ser señalada para habilitar su identificación para una subsecuente corrección de errores.

Las técnicas de control de entrada abarcan:

- Bitácora de transacciones.- Una bitácora de transacciones contiene una bitácora de actualizaciones de toda la base de datos. La bitácora puede ser mantenida manualmente o ser proporcionada por medio de un mecanismo automatizado. Una bitácora de transacciones se concilia con el número de documentos fuente recibidos para verificar que el total de transacciones fueron ingresadas.

- Conciliación de datos.- Los controles son necesarios para asegurar que el total de datos

recibidos son registrados y adecuadamente procesados.

- Documentación.-

  . Procedimientos de usuario

  . Documentos de entrada y

  . Control de datos

- Corrección de errores.-

  . Bitácora de errores

  . Tiempo de corrección

  . Aprobación de correcciones

  . Archivos en suspenso

  . Archivos de errores

  . Validación de correcciones

- Bitácora de transmisión.- Incluye la transmisión y recepción de datos.

- Cancelación de documentos fuente.- Son necesarios los procedimientos de cancelación de documentos para evitar la duplicidad de ingreso de información.

3 **PROCEDIMIENTOS DE CONTROL SOBRE ARCHIVOS DE DATOS**

Los controles sobre archivos deben asegurar que solamente ocurran procesos autorizados para almacenar datos.

Los tipos de control sobre archivos de datos son:

Recálculos manuales.- Los cálculos automáticos deben ser muestreados y recalculados manualmente para

asegurar que las aplicaciones de entrada son adecuadamente procesadas.

Edición.- Asegura que los datos de entrada cumplan los criterios predeterminados para lograr una oportuna identificación de errores potenciales.

Totales de control (totales run-to-run).- verifican que todos los datos transmitidos sean leídos y procesados en cada ejecución.

Límites de razonabilidad.- Los límites pueden ser predeterminados para calcular montos, cualquier cálculo que exceda el límite específicado debe ser rechazado para investigaciones posteriores.

Conciliación de totales de archivo.- La conciliación debe ejecutarse en una rutina base. Puede llevarse a cabo a través del uso de un contador mantenido manualmente, un registro de control de archivo o un control independiente de archivos.

Reportes de excepción.- Un reporte de excepción es generado por un programa que identifique transacciones o datos que son incorrectos. Estos elementos pueden no estar dentro de un rango determinado, o no cumplir con criterios especificados.

Controles de seguridad de archivos de datos.- Previenen accesos no autorizados a las aplicaciones. Estos controles no proporcionan la seguridad de la relación mantenida con la validación de datos, pero asegura que los datos almacenados no puedan ser alterados.

Verificación uno a uno.- Los documentos son agregados a una lista detallada de documentos procesados por el computador, esto es necesario para asegurar que todos los documentos han sido recibidos para proceso.

Campos pregrabados.- Ciertos campos de información son prestablecidos desde el ingreso para la reducción de errores en la captura.

Registro de transacciones.- Todas las actividades de ingreso de transacciones son registradas por el computador. Una lista detallada incluyendo fecha de ingreso, hora, identificación de usuario y localización de la terminal se genera para proveer una pista de auditoría. Esto también permite operaciones personales para determinar que transacciones han sido concluídas. Ello ayuda a decrementar el tiempo de investigación cuando sea necesario así como el tiempo de recuperación si ocurre una falla en el sistema.

3.1 Autorización para Actualización y Mantenimiento de Archivos

Es necesaria la autorización para actualizar y mantener archivos para asegurar que los datos almacenados son adecuadamente salvaguardados, correctos y actualizados. Los programas de aplicación pueden contener restricciones de accesos. La seguridad adicional provee niveles de autorización adicionalmente a pistas de auditoría sobre mantenimiento de archivos.

3.2 Validación y Edición de Datos

Los procedimientos deben ser establecidos para asegurar que los datos de entrada sean validados y editados tan cerca al punto de origen como sea posible. Formatos de entrada preprogramados aseguran que los datos sean ingresados en el campo y en la forma correcta. Si los procedimientos de entrada permiten supervisar la edición y validación de datos, puede existir una bitácora automática. Esta bitácora debe ser revisada por un supervisor diferente al que previamente revisó.

3.3 Proceso de Imagen Antes y Después

El proceso de imagen es recomendable cuando el volúmen de documentos a procesar es muy alto, los documentos representan montos importantes, los servicios a clientes son de considerable impacto, los documentos son procesados en múltiples pasos o varias estaciones y transacciones que son necesarias por un período de tiempo relativamente largo.

3.4 Actualización y Mantenimiento de Reportes de Error

Procedimientos de control deben ser implantados para asegurar que todos los reportes de error son adecuadamente verificados, conciliados y reingresados en un tiempo razonable. La corrección de errores debe ser revisada y autorizada por personal diferente al que inicio la transacción para asegurar la segregación de funciones.

3.5 Retención de Documentos Fuente

Los documentos fuente deben ser retenidos por un periodo de tiempo suficiente para permitir la recuperación, reconstrucción o verificación de datos. Las políticas relativas a la retención de documentos deben ponerse en vigor donde los departamentos origen deben mantener copias de los documentos fuente y asegurar que solamente personal autorizado tenga acceso. Cuando sea conveniente o aplicable, la documentación fuente debe ser destruída en un ambiente controlado y seguro.

3.6 Etiquetación Interna y Externa

Las etiquetas internas y externas son imprescindibles para asegurar que los datos correctos son cargados para los procesos correspondientes. Las etiquetas externas proveen el nivel básico para asegurar que se esta cargando el correcto medio de datos para su procesamiento. Las etiquetas internas incluyen registros de encabezados de archivo, proporcionando una segunda seguridad de que los datos cargados no son equivocados.

3.7 Uso de la Versión Correcta

El uso de la versión del sistema de aplicación correcta, asegura que todos los datos son procesados consistentemente. Cuando nuevas versiones de aplicación son recibidas, ellas deben ser establecidas en el área productiva, solamente cuando la autorización correspondiente ha sido recibida.

4 PROCEDIMIENTOS DE CONTROL SOBRE PROCESAMIENTO

4.1 Recálculos Manuales

Una muestra de transacciones puede ser recalculada manualmente para asegurar que el proceso está cumpliendo la tarea asignada.

4.2 Edición

Un verificador de edición es una rutina o instrucción en programa que prueba la validación de entradas en una aplicación.

4.3 Totales de Control

Proveen la facilidad de conciliar datos que han sido utilizados para actualizar otras aplicaciones. La conciliación asegura que todos los datos leídos fueron escritos en el archivo.

4.4 Límites de Razonabilidad

Una verificación de cálculos a través del uso de límites predefinidos proporciona la seguridad de que los montos calculados no han sido incorrectamente aplicados. Cualquier transacción que exceda el límite puede ser rechazada para posteriores investigaciones.

5 PROCEDIMIENTOS DE CONTROL SOBRE SALIDAS

5.1 Catalogación y Almacenamiento de Formas Negociables y Críticas en un Lugar Seguro

Formas negociables o críticas deben ser catalogadas y resguardadas para proporcionar una adecuada protección contra robo o daño. Las formas catalogadas deben ser rutinariamente conciliadas para inventariar su existencia y cualquier discrepancia debe ser investigada.

5.2 Generación Automática de Instrumentos Negociables, Formas y Firmas

La generación de instrumentos negociables, formas y firmas debe ser rígidamente controlada. Un lista detallada de las formas generadas debe ser comparada contra las formas físicas recibidas. Todas las excepciones, rechazos, y mutilaciones deben ser aclaradas.

5.3 Autorización de la Distribución

El acceso a la distribución de reportes puede comprometer la confidencialidad. La distribución debe ser adecuadamente controlada ya que las rutas de acceso pueden algunas veces ser descubiertas a través de la revisión de reportes. Los reportes que contienen información crítica deben ser impresos bajo condiciones controladas y de seguridad. La disposición de salidas impresas debe también ser adecuadamente asegurada para prevenir accesos no autorizados.

5.4 Balanceo y Conciliación

Las salidas impresas de los programas de aplicación deben ser rutinariamente balanceados contra los totales de control. Pistas de auditoría deben ser provistas para facilitar el seguimiento de transacciones procesadas y la conciliación de datos.

5.5 Manejo de Salidas Erróneas

Procedimientos para reportar y controlar errores contenidos en la salida impresa del programa de aplicación deben ser establecidos. El reporte de errores debe oportunamente ser entregado al departamento origen para la revisión y correción de errores.

5.6 Verificación de la Recepción de Reportes

Para proporcionar seguridad de que los reportes críticos son adecuadamente distribuídos, el receptor

deberá firmar una bitácora para evidenciar la recepción de los reportes.

6 TIPOS DE DOCUMENTACION DE APLICACIONES

6.1 Diagramas de Flujo de Sistemas

Los diagramas de flujo de sistemas son representaciones gráficas de la secuencia de operaciones en un sistema de información. Los diagramas muestran los datos desde el documento fuente a través del computador hasta la distribución final a los usuarios. Los símbolos utilizados deben ser los estándares internacionalmente aceptados. Los diagramas de flujo deben ser actualizados cuando sea necesario.

6.2 Narrativas de Sistemas

Las narrativas de sistemas proporcionan una explicación general del diagrama de flujo de sistemas, con explicaciones claves de puntos de control e interfases de sistemas.

6.3 Diagramas de Flujo de Programas

Los diagramas de flujo de programas muestran la secuencia de instrucciones en un programa individual o subrutina. Los símbolos usados deben ser los estándares internacionalmente aceptados. Los diagramas de flujo de programas deben ser actualizados cuando sea necesario.

6.4 Narrativas de Programas

Proporcionan una explicación detallada del diagrama de flujo del programa, incluyendo puntos de control y cualquier entrada externa.

6.5 Manuales de Usuario

Son escritos para los individuos que interactúan con el computador a nivel programa de aplicación. Los programadores, operadores y otro personal técnico no son usuarios. Sin embargo, el manual de usuario no debe contener código fuente y explicaciones de restricciones de acceso. Los manuales de usuario deben contener instrucciones detalladas relativas al uso de la aplicación diaria, identificando procedimientos para autorización de transacciones, manejo de documentación, correción de errores e interpretación de reportes.

6.6 Descripción de Registros, Pantallas y Reportes

La descripción de registros proporciona información relativa al tipo de registro, el tamaño y que datos son contenidos en el registro. La descripción de pantallas y reportes describen que información es proporcionada y es necesaria para el ingreso.

6.7 Diccionario de Datos

Un diccionario de datos es una base de datos que contiene el nombre, tipo, rango de valores, fuente y autorización para el acceso a cada elemento dentro de una base de datos. Esto también indica los datos utilizados por cada programa de aplicación, así cuando un cambio en una estructura de datos es contemplado, una lista de programas que afectan puede ser generada. El diccionario de datos puede ser independiente al sistema de información y usado por la gerencia para propósitos de documentación o para controlar la operación de la base de datos.

7 TECNICAS DE AUDITORIA Y EVALUACION

7.1 Revisión de la Documentación de Aplicaciones para Obtener un Entendimiento de los Componentes Funcionales de la Aplicación

La documentación de aplicaciones proporciona un entendimiento preliminar de una aplicación. Si una aplicación es adquirida, se deben proporcionar

manuales técnicos y de usuarios los cuales deben ser revisados. Cualquier cambio a las aplicaciones debe ser oportunamente documentado. La siguiente documentación también debe ser revisada para obtener un entendimiento del desarrollo de la aplicación:

- Documentación de la metodología de desarrollo de sistemas.- Este documento incluye el análisis de costo/beneficio y requerimientos de usuario.

- Especificaciones del diseño funcional.- Este documento provee una explicación detallada de la aplicación. Un entendimiento de los puntos claves de control debe presentarse durante la revisión de las especificaciones de diseño.

- Cambios a programas.- La documentación de cualquier cambio debe estar disponible para revisión. Cualquier cambio debe proporcionar evidencia de autorización y debe contar con referencias cruzadas al código fuente.

- Manuales de usuario.- Una revisión del manual de usuario proporciona el fundamento para el entendimiento de como el usuario esta utilizando la aplicación. Frecuentemente, la debilidad en el control puede ser notada desde la revisión de este documento.

- Documentación técnica de referencia.- Esta documentación incluye a cualquier manual técnico tanto de aplicaciones adquiridas como desarrolladas en las propias instalaciones. Las reglas de acceso lógico son usualmente incluidas en estos documentos.

7.2 Analizar el Flujo de Transacciones a través del Sistema

Un diagrama de flujo proporciona esta información relativa a los puntos de proceso claves. Los puntos donde las transacciones son ingresadas, procesadas y presentadas deben ser revisados por la posibilidad de que existan debilidades de control.

7.3 Preparación de un Modelo de Riesgo para Analizar los Controles de Aplicación

El modelo de riesgo proporciona información relativa a los riesgos inherentes de un aplicación. Un modelo de riesgo puede basarse en muchos factores, incluyendo:

- La calidad del control interno
- Condiciones económicas
- Cambios recientes a los sistemas (contables)
- Tiempo transcurrido desde la última auditoría
- Complejidad de las operaciones
- Cambios recientes a posiciones claves
- Cambios en operación o en el medio ambiente
- Tiempo de existencia
- Competencia en el medio
- Resultados de la última auditoría
- Rotación de personal
- Volúmen de transacciones
- Volúmenes monetarios
- Impacto de los cambios reglamentarios
- Transacciones críticas
- Impacto de aplicaciones erróneas

7.4 Observar y Probar los Procedimientos de Usuario

- Segregación de funciones.- Asegura que los usuarios no tengan la capacidad de desarrollar más de una de las siguientes funciones de ingreso de información: elaboración, autorización, verificación o distribución. Observar, revisar la descripción de trabajos y revisar los niveles de autorización, proporcionan información relativa a la existencia del cumplimiento de la segregación de funciones.

- Autorización del ingreso.- Evidencia de la autorización del ingreso puede ser lograda, vía autorización escrita en los documentos de entrada o con el uso de un password único. Esto puede ser probado mediante una muestra de documentos fuente, observando su debida autorización o revisando la ruta de acceso al sistema.

- Balanceo.- Debe ser llevado a cabo para verificar que los totales de control y otros totales de aplicación son conciliados en un tiempo considerable. El balanceo puede ser probado volviendo a ejecutar o revisando conciliaciones anteriores.

- Control y corrección de errores.- Los reportes de error proporcionan evidencia de la adecuada revisión, investigación oportuna corrección y reingreso de la información. Los errores de ingreso y rechazos deben ser revisados previamente a su reingreso. La revisión gerencial y la autorización de las correcciones debe quedar evidenciada. La prueba de ello puede desarrollarse volviendo a procesar o revisando correcciones de errores pasados.

- Distribución de reportes.- Los reportes críticos deben ser emitidos y mantenidos en un área restringida y distribuídos en una forma autorizada. El proceso de distribución puede probarse observando y revisando las bitácoras de distribución de salidas. El acceso en línea a reportes debe ser restringido. Este acceso puede ser probado a través de la revisión de las reglas de acceso.

7.5 Revisión y Prueba de las Capacidades y Autorizaciones de Acceso

- Tablas de control de acceso.- Proporcionan información referente a niveles de acceso individuales. Los accesos deben basarse en la descripción del trabajo y proporcionar una adecuada segregación de funciones. La prueba puede llevarse a cabo a través de la revisión de las reglas de acceso para asegurar que han sido propuestas y supervisadas por la gerencia.

- Reportes de actividad.- Proveen detalles por usuario del volúmen de actividades y horas. Deben ser revisados para asegurar que las actividades ocurran solamente durante las horas normales de operación.

- Reportes de violación.- Indican cualquier intento de acceso no autorizado. Deben indicar la localización de la terminal, fecha y hora cuando el acceso fué intentado. Este reporte debe contener evidencia de la revisión gerencial. Las pruebas pueden incluir la revisión del seguimiento de los procedimientos.

7.6 **Seleccionar el Tipo Apropiado de CAAT (Computer Aided Audit Technics - Técnicas de Auditoría Asistidas por el Computador)**

Método de Datos de Prueba (Test Data Method).- Verifica la exactitud del proceso de un sistema de aplicación automatizado mediante la ejecución de los mismos, usando un conjunto de datos de entrada especialmente preparados que producen resultados preestablecidos. El método constituye un procedimiento de verificación de programas y aplicaciones. Esta es una buena técnica para utilizarse inicialmente en la verificación de programas porque las pruebas pueden ser expandidas incrementalmente. Procedimientos especiales no son usualmente requeridos. El método de datos prueba se limita a la verificación y evaluación del procesamiento y no es una técnica apropiada para la verificación de los datos en producción. No se proporciona evidencia concerniente a la totalidad o exactitud de los datos ingresados a la producción o archivos maestros.

Evaluación de Sistemas con una Caso Base (BCSE, Base Case System Evaluation).- Es una técnica que aplica un grupo estándar de datos (entrada, parámetros y salida) para probar un sistema de aplicación. Este grupo de datos, es establecido con base al criterio de que el sistema de aplicación funciona correctamente. Este proceso de prueba es más ampliamente utilizado como una técnica de validación de un sistema de aplicación en producción y se usa frecuentemente para probar programas durante su desarrollo, para demostrar la satisfactoria operación del sistema previo a su instalación y para verificar su continuidad durante el periodo de vida del mismo.

Instalación de Prueba Integrada (ITF Integrated Test Facilities).- Es una técnica para revisar aquellas funciones internas de una aplicación automatizada. Se utilizan datos de prueba para comparar resultados del proceso ITF con los datos precalculados. El método es utilizado frecuentemente para probar y verificar sistemas de aplicación muy grandes cuando no es práctico separar el sistema en ciclos. La técnica ITF es utilizada para verificar y evaluar procesos automatizados y es de valor limitado para la verificación de datos en producción o archivos de datos. Se proporciona evidencia limitada concerniente a la totalidad y exactitud de los datos ingresados a producción o archivos maestros.

Simulación en Paralelo.- Es el uso de uno o más programas para procesar archivos de datos "vivos" y simular procesos normales de aplicación. Es opuesto al método de datos de prueba y al ITF, los cuales procesan datos de prueba a través de programas en producción. El método de simulación en paralelo, procesa datos de prueba productivos a través de programas de prueba. Los programas de la simulación en paralelo incluyen solamente las aplicaciones lógicas, cálculos y controles que son relevantes para cubrir objetivos específicos de auditoría, como resultado, los programas de simulación son usualmente mucho menos complejos que sus equivalentes en aplicación. Segmentos de una aplicación muy grande consistente de varios programas, pueden ser frecuentemente simulados para propósitos de auditoría, con programas de simulación en paralelo. La simulación en paralelo permite al auditor verificar en forma independiente, procedimientos complejos y críticos de un sistema de aplicación.

Selección de Transacciones.- La técnica de auditoría de selección de transacciones usa un programa independiente para monitorear y seleccionar transacciones para la revisión de auditoría. El método permite al auditor examinar y analizar un volúmen de transacciones y errores, determinados mediante muestreo estadístico. El software de auditoría para selección de transacciones es totalmente independiente al sistema de aplicación y es generalmente controlado mediante parámetros. No se requiere la alteración del sistema de aplicación. Esta técnica es especialmente apropiada para el monitoreo y muestreo de transacciones en sistemas de aplicación complejos.

Módulos de Auditoría Integrados.- Utiliza uno o más módulos especialmente programados para la recopilación de datos e integrados al sistema de aplicación para seleccionar y grabar datos para su análisis y evaluación. Los módulos de recopilación de datos son insertados en el sistema de aplicación en puntos determinados por el auditor, definiendo también, el criterio de selección y grabación. Subsecuente a la recopilación, otro método automatizado o manual debe utilizarse para analizar los datos obtenidos.

A comparación de otros métodos de auditoría, esta técnica utiliza código en línea (por ejemplo, el programa de aplicación que ejecuta la función de recopilación de datos, al mismo tiempo lleva a cabo sus funciones normales). Esto tiene dos importantes consecuencias para el auditor: el código en línea asegura la disponibilidad de una comprensiva o una muy especializada muestra de datos (los módulos son estratégicamente colocados para accesar a cada dato procesado). Esta técnica para una sistema ya existente es más costosa que implantar la programación de auditoría durante el desarrollo de sistemas, por ello es preferible para el auditor especificar sus requerimientos mientras el sistema esta siendo diseñado.

Registros Extendidos.- Los registros extendidos son una técnica que reune, por medio de uno o varios programas especiales, todos los datos significativos que afectan el procesamiento de una transacción individual. El registro extendido incluye datos de todos los sistemas de aplicación que contribuyen al procesamiento de una transacción.

Con esta técnica, el auditor no necesita revisar muchos archivos para determinar como una transacción específica fué procesada. Con los registros extendidos, los datos son consolidados de diferentes periodos y diferentes sistemas de aplicación, por lo que una pista de auditoría de una transacción completa está físicamente incluída en un registro. Ello facilita las pruebas de cumplimiento de las políticas y procedimientos de la organización.

Software Generalizado de Auditoría.- Es la técnica más ampliamente utilizada para auditar sistemas de aplicación. Esta técnica permite al auditor analizar independientemente un archivo de un sistema de

aplicación. Varios paquetes de auditoría, por su difundida utilización e historia, son ultraconfiables, altamente flexibles y extensiva y correctamente documentados. El software de auditoría generalmente incluye estratificaciones, comparaciones entre archivos, sumarizaciones, criterios de extracción, selección de muestras mediante muestreo estadístico y ejecución de cálculos sobre diversos datos contenidos dentro de varios archivos. Esta gama de capacidades están disponibles para la aplicación de pruebas sustantivas por parte del auditor, generalmente, este método de auditoría es utilizado para verificar archivos de datos. Pequeñas facilidades se presentan para probar la lógica del sistema, esta va implícita en los resultados mostrados en los archivos de datos.

Snapshot.- Tanto el auditor y el personal de procesamiento normalmente se enfrentan ante la dificultad de la reconstrucción del proceso para la toma de decisiones. La causa corresponde a la falla para obtener todos los elementos involucrados en el proceso. Snapshot es una técnica que toma una fotografía de las partes de la memoria de la computadora que contiene los elementos de datos involucrados en el proceso automatizado de toma de decisiones al momento en que la decisión es tomada. El resultado del snapshot son impresiones en formato de reporte para la reconstrucción del proceso de toma de decisiones.

La técnica de auditoría de snapshot ofrece la capacidad de listar todos los datos participantes en un proceso de toma de decisones. La técnica requiere la lógica para ser preprogramada en el sistema. Un mecanismo, usualmente un código especial en el registro de transacciones, es añadido para enviar a impresión los datos en cuestion para su análisis.

Esta técnica ayuda al auditor a responder preguntas sobre porque el sistema de aplicación produce resultados cuestionables. Ello proporciona información para explicar porque una decisión en particular fué desarrollada por el sistema. Snapshot utilizada en conjunto con otras técnicas de auditoría, proveen la determinación de qué resultados ocurrirán si un cierto tipo de dato se ingresa a procesamiento al sistema. También es una ayuda invaluable para el personal de desarrollo de sistemas en la depuración del sistema porque proporciona un vaciado de la memoria de la computadora.

Seguimiento (Tracing).- Una técnica de auditoría tradicional en un medio ambiente manual, es el seguir la ruta de una transacción durante el procesamiento. Por ejemplo, un auditor recolecta una orden con su respectiva recepción dentro de la organización y sigue el flujo de estación de trabajo, en estación de trabajo. El auditor consulta a los empleados involucrados en las acciones llevadas a cabo en un paso en particular dentro del ciclo de procesamiento. Con el entendimiento de las políticas y procedimientos de la organización, el auditor puede juzgar si estos se están cumpliendo adecuadamente. Por el tiempo invertido en el seguimiento a través del ciclo de procesamiento, el auditor obtiene una buena apreciación del flujo de trabajo através de la organización. En un ambiente de procesamiento de datos, no es posible seguir la ruta de una transacción a través del ciclo de procesamiento solamente por el seguimiento del flujo en papeles de trabajo. Muchas de las funciones ejecutadas por los empleados y el movimiento de copias de documentos son remplazados por procesos de datos electrónicos.

El seguimiento es una técnica de auditoría que proporciona al auditor la capacidad de llevar a cabo un seguimiento electrónico de datos en un sistema de aplicación. El objetivo de auditoría del seguimiento es verificar el cumplimiento de las políticas y procedimientos mediante la comprobación, a través de la examinación de la ruta seguida por una transacción dentro de un programa o mediante el conocimiento de que transacción fué procesada. Ello puede ser utilizado para verificar omisiones. El seguimiento muestra que instrucciones han sido ejecutadas. Las instrucciones en un programa representan los pasos en un proceso, los procesos que han sido ejecutados pueden ser determinados por el resultado del seguimiento. Una vez que el auditor conoce que instrucciones han sido ejecutadas en un programa, puede llevar a cabo un análisis para determinar si el procesamiento es conforme a los procedimientos de la organización.

Mapping.- Es la técnica para determinar la extensión de prueba de sistemas y para identificar la lógica de programas específicos que no necesariamente tienen que ser pruebas.

Mapping es ejecutado por un software que sirve como herramienta de medición de análisis a programas de computadora, durante la ejecución, para indicar el

estado de un programa en el tiempo que debe ser ejecutado. El software puede ser una herramienta para medir o determinar la cantidad de CPU que consume por cada sección de programa.

El propósito original del mapping es para ayudar al programador del computador a asegurar la calidad de sus programas. Asimismo, el auditor puede utilizar ese pequeño software como herramienta para encontrar código no ejecutable.

Este análisis puede proporcionar que el auditor tenga conocimiento de la eficiencia de la operación de un programa y pueda revelar que sección de programa no cumple con los procedimientos establecidos, incluye también la ejecución de accesos no autorizados.

Diagrama de flujo de datos (Flowcharting).- En un medio ambiente de negocios complejo es difícil de entender completamente todos los sistemas de control de una organización con este contexto de operaciones. Una gráfica técnica o un diagrama de flujo para simplificar la identificación y la interrelación de controles, puede ser de mayor ayuda en la adecuada evaluación de esos controles y en la determinación del impacto del cambio a los sistemas en el que incluye los perfiles de control. Los diagramas de flujo facilitan la exploración de controles para análisis del sistema, para auditoría externa o personal no familiarizado, mismo que da especificaciones de la operación del sistema, ellos también ayudan en investigar que controles están operando.

La técnica de auditoría de diagramas de flujo proporciona la documentación necesaria para explicar los sistemas de control. Algunas veces la información de los controles de una organización esta seccionada, esto hace que sea más difícil obtener una clara idea de los controles de operación de la misma. La ventaja de mantener en diagramas los controles incluye el uso de varios niveles de segregación, facilitando así el entendimiento de estos.

Carga y descarga de datos (Uploading and Downloading Data).- Los datos pueden ser cargados desde un mainframe a una PC para permitir un mayor análisis de las transacciones seleccionadas bajo criterios establecidos (downloading). La manipulación de datos

puede ser cargada nuevamente al mainframe (Uploading).

CASE (Computer Aided Software Engineering).- Se refiere al uso de paquetes de software para ayudar en las fases del desarrollo de sistemas de información. El análisis, diseño, programación y documentación son proporcionados mediante su utilización. Los cambios introducidos en un diagrama CASE, actualizan automaticamente todos los demás diagramas relacionados. CASE puede instalarse en una microcomputadora para facilitar su acceso.

Sistemas expertos.- Son el más prevaleciente tipo de sistemas que se logran de la investigación de la inteligencia artificial. Un sistema experto se construye de un conjunto de reglas jerárquicas que son adquiridas de expertos en estos campos. Una vez provista la entrada el sistema debe permitir la definición de la naturaleza del problema y proveer recomendaciones para la solución de problemas.

CAPITULO VI

OBTENCION, EVALUACION DE EVIDENCIA Y REPORTES DE AUDITORIA

VI OBTENCION, EVALUACION DE EVIDENCIA Y REPORTE DE AUDITORIA

OBJETIVO

El auditor entenderá los componentes básicos de un reporte de auditoría y como comunicar adecuadamente los hallazgos de auditoría a la administración.

INTRODUCCION

La satisfación de una auditoría depende de una comunicación efectiva y unos resultados adecuadamente evidenciados. Los reportes de auditoría involucran las tres siguientes funciones:

- Documentación interna
- Reporte de auditoría
- Retroalimentacion para la auditoría y la gerencia

Las funciones de los reportes de auditoría son completamente enfocados para permitir a los lectores, relacionar la información con sus propias actividades o proyectos.

La documentación interna consiste de papeles de trabajo y otros documentos pertenecientes a una auditoría específica. Sin embargo la compilación de papeles de trabajo de auditoría no es el objetivo de una auditoría.

El reporte de auditoría, como ya se mencionó, debe incluir una declaración de opinión relativa a los hallazgos del auditor de sistemas de información. El auditor debe también comunicar cualquier reserva o calificación con respecto a la auditoría. Estos pueden tomar la forma de controles o procedimientos examinados que fueron encontrados como adecuados o inadecuados. El balance del reporte de auditoría debe soportar la conclusión, y la evidencia general obtenida durante la auditoría debe proporcionar un alto nivel de soporte.

El auditor frecuentemente presenta los resultados de su trabajo a varios niveles de dirección. El auditor de sistemas debe tener un conocimiento completo de las técnicas de presentación necesarias para comunicar estos resultados.

1 TECNICAS DE OBTENCION DE EVIDENCIA

1.1 Análisis de las Estructuras de Organización de los Sistemas de Información

Un fuerte plan de organización con una adecuada segregación de funciones es un control clave en una función de sistemas de información. El auditor de sistemas debe entender los controles organizacionales generales y poder evaluarlos en la organización bajo auditoría.

1.2 Analizar las Normas de Documentación de los Sistemas de Información

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

- Documentos de iniciación del desarrollo de sistemas
- Especificación de diseño funcional,
- Historia de cambios de programa y
- Manuales de documentación de usuario

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

1.3 Analizar la Documentación de los Sistemas

El auditor puede analizar la documentación de un sistema dado y determinar si sigue las normas de documentación de la organización. Además, el auditor debe comprender el enfoque más reciente para

desarrollar sistemas, tales como CASE o prototipos, y como se construye la documentación. El auditor debe reconocer otros componentes de la documentación de los sistemas de información tales como especificaciones de bases de datos, descripción de archivos o listados de programas autodocumentados.

1.4 Entrevistar al Personal Apropiado

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

1.5 Observar el funcionamiento de operaciones y empleados

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

El auditor 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.

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

1.6 Seleccionar y Examinar Controles Clave

El análisis inicial de un sistema de información por parte de un auditor de sistemas de información debe identificar los controles clave, entonces decidirá exáminar 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, identificará los puntos de control clave en la aplicación. La identificación permitirá desarrollar una comprensión preliminar a través de pruebas de cumplimiento de aquellos controles para determinar si están trabajando como se desea. Los resultados de estas pruebas de cumplimiento permitirán diseñar pruebas de cumplimiento o sustantivas más extensas.

1.7 Aplicar Técnicas de Muestreo

El auditor de sistemas de información debe tener un profundo entendimiento de las técnicas de muestreo de auditoría, incluyendo procedimientos de muestreo estadístico de atributos o de variables. El auditor debe entender cuando 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 o un grupo de controles relacionados (los atributos). Un ejemplo de un atributo que puede ser examinado es la firma de aprobación en las formas de solicitud de acceso a la computadora.

- Muestreo de variables

  El cual es también conocido como estimación monetaria (dólar) 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 determinada. 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.

1.8 Técnicas de Auditoría Asistidas por el Computador (CAAT)

El auditor de sistemas de información debe tener un profundo conocimiento de las técnicas asistidas por el computador y donde 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 prueba integradas. Además de seleccionar la técnica apropiada, el auditor debe entender la importancia de documentar los resultados de tales puebas para propósitos de evidencia de auditoría.

Ejemplos del uso de técnicas CAAT son las siguientes:

- Utilización de un generador de datos de prueba para preparar un lote de prueba para verificar la lógica de los programas de aplicación.

- Utilización de sistemas expertos residentes en el computador que invoquen módulos de software de análisis dentro del sistema operativo o sistema de seguridad.

- Utilización de utilerías estándar residentes en paquetes de software que especifiquen el estatus de los parámetros usados para instalar el paquete.

- Utilización de paquetes de bibilioteca de software para verificar la integridad y la corrección de los cambios a programas.

2. EVALUACION DE LAS FORTALEZAS Y DEBILIDADES DE LA AUDITORIA

Despúes 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 para entonces poder 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 de EDPAF NO. 8 "Debido cuidado profesional" es particularmente importante para el auditor al evaluar las fortalezas y debilidades.

El auditor de sistemas de información debe evaluar los resultados de la evidencia recopilada de conformidad con los requerimientos y objetivos de control establecidos durante la etapa de planeación. Esto exige un considerable juicio profesional ya que frecuentemente los controles no son claros.

2.1 Información Relevante y Periférica

El auditor recopila una diversidad de evidencia durante la auditoría. Alguna puede ser relevante para los objetivos de la auditoría, mientras otra puede ser considerada periférica. El auditor debe enfocarse a los objetivos globales de análisis y no en la naturaleza de la evidencia recopilada. El buen juicio será aplicado para determinar que material es exactamente apropiado para los objetivos perseguidos en la auditoría y cual no es específicamente relevante.

2.2 Consideración de los Controles Compensatorios y de 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 de control. En algunas ocasiones un control fuerte puede compensar a un control débil en otra

área. Por ejemplo, aún si el auditor encuentra debilidades en un reporte de errores de transacción de sistemas, puede encontrar que un proceso detallado del balanceo manual sobre todas las transacciones, compensa la debilidad en el reporte de errores. El auditor debe estar consciente de compensar controles en áreas donde han sido 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 un 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 encabezados de la cinta. Esta es una debilidad de control, sin embargo, el auditor puede encontrar procedimientos muy fuertes de inicialización, modificación y montaje de las cintas en el centro de cómputo , que sólo las cintas correctas pueden ser montadas. Si los controles sobre los procedimientos 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 magnéticas para controlar el acceso físico. Si hay también un guardia adentro de la puerta el cual pide a los empleados mostrar su tarjeta o identificación, esto sería un control superpuesto. Cualquiera de los dos controles pueden ser adecuados para restringir el acceso y los dos se complementan.

2.3 Considerar la Interrelación de Controles

El auditor de sistemas de información realizará una variedad de procedimientos de prueba y evaluará como éstos se relacionan.

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

2.4 Determinar la naturaleza de las operaciones efectivas y eficientes

El auditor debe analizar la evidencia reunida durante la auditoría 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. Se deben evaluar las fortalezas y debilidades de los controles para así determinar si estos son efectivos para cumplir con los objetivos de control establecidos como parte del proceso de planeación de auditoría.

2.5 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 para este tipo de análisis, el cual permite al auditor estudiar una variedad de datos aleatorios y determinar si representan una tendencia. La naturaleza de la técnica de análisis dependerá de la evidencia que se examine. Sin embargo, el auditor debe tener un completo entendimiento de las técnicas analíticas, tal como el análisis de regresión.

2.6 Juzgar la importancia de los Hallazgos.

Este es un asunto clave para presentar hallazgos decisivos en un reporte de auditoría 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 significativo para la administración del sitio remoto, pero no ser necesariamente esencial para la administración en las oficinas principales. Sin embargo, tal vez existen otros temas en la sede remota que sean significativos para la administración.

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

3 REPORTE DE AUDITORIA

Los reportes de auditoría son el producto final del auditor. Este es el vehículo que el auditor usa para reportar sus hallazgos y recomendaciones a la administración. El formato exacto de un reporte de auditoría variará por la organización. Sin embargo, el auditor habilidoso entenderá los componentes básicos de un reporte de auditoría y como comunicar adecuadamente los hallazgos a la administración. El auditor debe entender las normas generales de EDPAF "Informe de la extensión de la auditoría" y el "Reporte de hallazgos y conclusioneu".

3.1 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.

3.2 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 del 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 de que incluir o excluir en el reporte de auditoría. El auditor debe entender las normas generales de EDPAF sobre independencia.

3.3 Restricciones sobre Recomendaciones a Implantar

El auditor debe reconocer que la administración puede o no implantar todas las recomendaciones de auditoría inmediatamente. Otros factores pueden retrasar tales acciones, por ejemplo, se pueden 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 las recomendaciones estén instaladas adecuadamente, ambas pueden ser instaladas juntas.

El auditor debe discutir las recomendaciones y la fecha planeada de implantación durante el proceso de liberación del reporte de auditoría. Mientras el auditor debe darse cuenta de las diversas restricciones tales como, limitación de personal, presupuestos y de otros proyectos, puede limitar la implantación inmediata, la administración debe desarrollar un firme programa para las acciones correctivas. Si es apropiado, el auditor puede reportar a la alta administración sobre el progreso de la implantación de estas recomendaciones.

3.4 Importancia Relativa de las Debilidades

Un reporte de auditoría incluirá una variedad de hallazgos, algunos de los cuales pueden ser bastante importantes, mientras otros son menores en naturaleza. En el seguimento del programa de la administración para implantar recomendaciones, el auditor debe considerar su relativa importancia.

3.5 Comunicar Resultados a la Administración y Comité 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 copias de todos los reportes de auditoría, de vez en cuando el auditor de sistemas de información encontrará asuntos que deberán ser llamados inmediatamente a su atención. El auditor debe sentirse libre para comunicar estos asuntos o preocupaciones a tal administración. Un intento de la administración prinicipal para negar el acceso del auditor limitaría la independencia de la función de auditoría.

3.6 Declaraciones de Opinión y Conclusión

Como se mencionó el reporte de auditoría debe incluir una declaración de opiniones con respecto a los hallazgos del auditor. Como está definido en las normas generales del EDPAF 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 o inadecuados. El balance del reporte de auditoría apoyará esta conclusión y la evidencia global reunida durante la auditoría proporcionará un mayor nivel de apoyo.

3.7 Técnicas de Presentación

El auditor frecuentemente será requerido para presentar los resultado del trabajo de auditoría a varios niveles de la administración. El auditor debe tener un completo conocimiento de la técnicas de presentación necesarias para comunicar estos resultados, las técnicas de presentación pudieran incluir lo siguiente:

- Un reporte fácil de leer, gramáticamente correcto y conciso que presente los hallazgos a la administración. La mayoría de los 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 anexos detallados pueden ser de naturaleza más

técnica ya que la gerencia de operaciones requiere los detalles para poder corregir las situaciones reportadas.

- Transparencias para retroproyector o diapositivas de 35mm generadas a tráves de paquetes de software graficador.

4 ACCIONES DE LA ADMINISTRACION PARA IMPLANTAR LAS RECOMENDACIONES.

Los auditores deben darse cuenta que auditar es un proceso continuo. 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 de seguimiento para determinar si las acciones correctivas prometidas han sido tomadas bajo las recomendaciones de la auditoría. La oportunidad del seguimiento dependerá del carácter crítico de los hallazgos y estarían sujetos al juicio del auditor de sistemas de información. Los resultados del seguimiento deben ser comunicados a los niveles de administración apropiados.

CONCLUSIONES

CONCLUSIONES

Como resultado de una Auditoría en Informática, el auditor detecta debilidades que afectan a la organización auditada en la efectividad y eficiencia de sus operaciones. Sin embargo, no es solo su responsabilidad el informar dichas debilidades, sino proponer soluciones proporcionando los medios y elementos con que se pueden minimizar, ello como un valor agregado de la auditoría hacia la organización. Asimismo, debe darse seguimiento a las soluciones elegidas a fin de asegurar su adecuada implantación, siendo una parte integral de la Auditoría en Informática.

Una vez cubierto el capitulado consideramos que se tendrán los elementos para poder identificar si con el establecimiento de la función de Auditoría en Informática se logra el cumplimiento de los objetivos de salvaguarda de activos, integridad de datos, efectividad y eficiencia de los sistemas y ambiente de control automatizados que operan en cada organización.

Actualmente en nuestro país la Auditoría en Informática se encuentra en su parte inicial y esta siendo apoyada por la Asociación Mexicana de Auditores en Informática (AMAI), tomando fuerza a medida que la tecnología se aplica en las organizaciones, haciendo más compleja la práctica de la auditoría tradicional, esto conlleva a que como auditores en informática se mantenga una capacidad técnica cada vez mayor. La EDPAF (Electronic Data Processing Auditors Fundation) a nivel internacional y en México su representante AMAI, se crearon con el objeto de promover la educación, comunicación, necesidades de desarrollo profesional e investigación en los campos interrelacionados de la auditoría e informática. Dichas organizaciones establecieron un programa para el otorgamiento de una certificación como auditores EDP. Los objetivos que se persiguen son:

- Desarrollar y mantener actualizados instrumentos de prueba que pudieran ser utilizados para evaluar la capacidad para realizar auditorías en informática,

- Proveer un mecanismo que permitiera motivar a los auditores en informática a mantener su capacidad y

supervisar el éxito de los programas de actualización, y

- Contribuir con la alta gerencia a crear una función de Auditoría en Informática sólida por medio de criterios para la selección y capacitación de personal.

Dicha certificación es conocida como CISA (Certified Information Systems Auditor) que constituye una calificación profesional donde se pone a prueba la habilidad del auditor para comprender el cuerpo común de conocimientos que exige la profesión. Los temas que se abarcan son:

- Normas, procedimientos y técnicas de auditoría
- Organización y administración de la función de informática
- Operación del centro de cómputo
- Acceso lógico, acceso físico y controles ambientales
- Continuidad de operaciones
- Desarrollo, adquisición y mantenimiento de software de sistemas
- Desarrollo, adquisición y mantenimiento de aplicaciones
- Sistemas de aplicación

Con el conocimiento profundo de estas áreas, se apoya a la consecución de los objetivos de una Auditoría en Informática

BIBLIOGRAFIA

BIBLIOGRAFIA

- Li, David H., Auditoría en Centros de Cómputo, México, Editorial Trillas, enero 1990.

- The EDP Auditors Foundation, Inc, The EDP Auditor Journal, Volume IV, 1990.

- PRICE WATERHOUSE, Serie de Guías de Auditoría, Sistemas de Información Computadorizados, Copyright 1988.

- Weber, Ron, EDP Auditing, Conceptual, Foundations and Practice, New York, Mc Graw Hill Book Co., Second edition, 1988.

- The Institute of Internal Auditors, Inc., Systems Auditability & Control, Control Practices, Altamonte Springs, Florida, fifth printing 1980.

- Jack, B. Mullen, The Practitioner's guide to EDP Auditing, New York of Finance, NYIF Corp, 1990.

- The EDP Auditors Foundation, Inc., General Standars for Information Systems Auditing, 1992.

- Murphy and X.L. Parker, Warren, Gorham & Lamont, Inc., Handbook of EDP Auditing, Boston, Ma., 1989.

- Robert Moeller, John Wiley & Sons, Inc., Computer Audit, Control and Security, New York, 1990.

- Auditors Foundation, Control Objectives: Publication of The EDP, Carol Stream, Ill., 1990.

- Hernández Jiménez, Ricardo, Administración de Centros de Cómputo, México, Editorial Trillas, primera edición, marzo 1988.

- Echenique García, José A., Auditoría en Informática, Apuntes, 1989.

- Instituto Mexicano de Contadores Públicos, Normas y Procedimientos de Auditoría, México, Décimotercera edición, enero de 1993.